FIG. 1

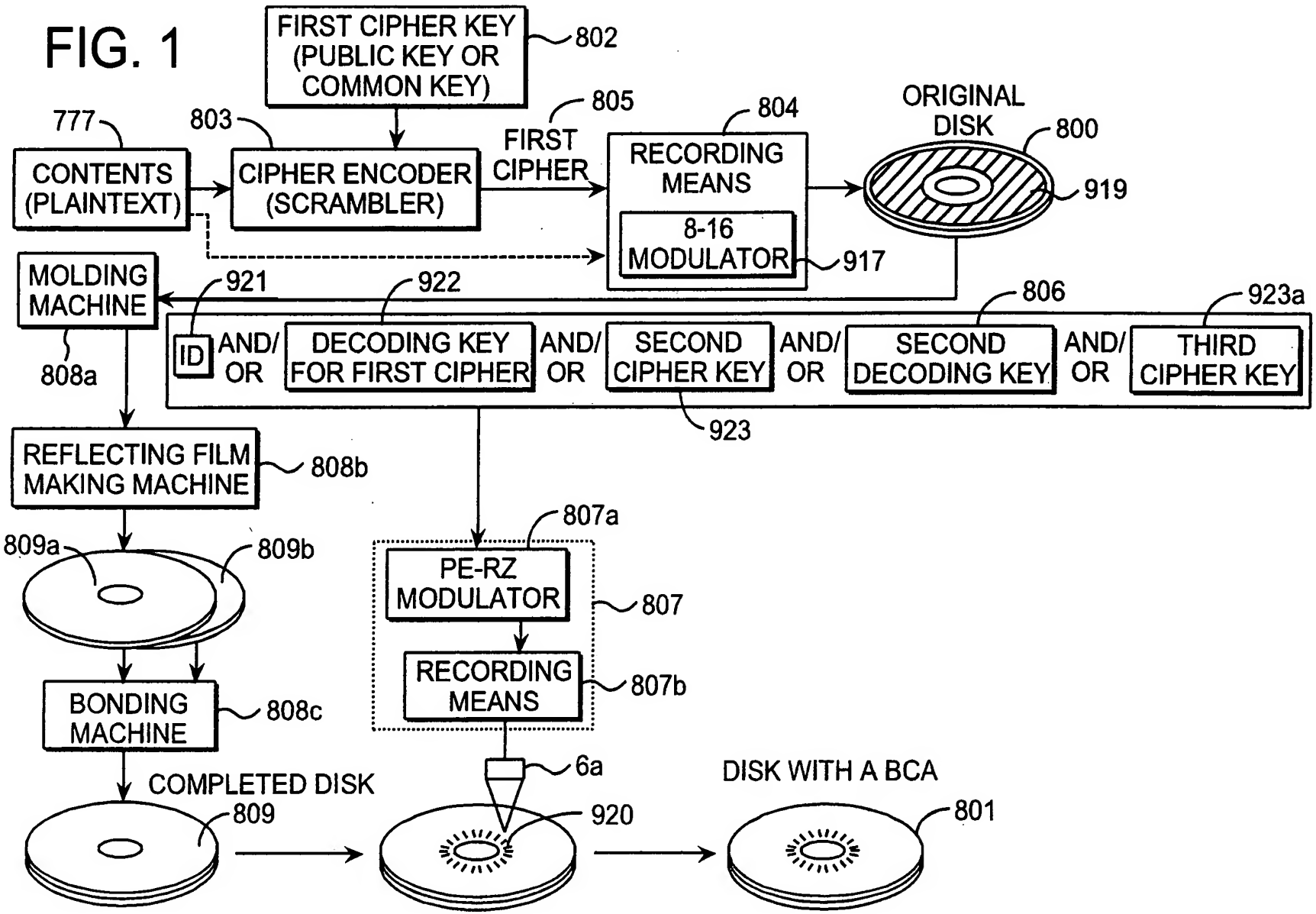

FIRST CIPHER KEY (PUBLIC KEY OR COMMON KEY)
802
777
803
805
804
ORIGINAL DISK
800
CONTENTS (PLAINTEXT)
CIPHER ENCODER (SCRAMBLER)
FIRST CIPHER
RECORDING MEANS
8-16 MODULATOR
917
919
MOLDING MACHINE
921
922
806
923a
808a
ID
AND/ OR
DECODING KEY FOR FIRST CIPHER
SECOND CIPHER KEY
SECOND DECODING KEY
THIRD CIPHER KEY
923
REFLECTING FILM MAKING MACHINE
808b
807a
809a
809b
PE-RZ MODULATOR
807
RECORDING MEANS
807b
BONDING MACHINE
808c
6a
COMPLETED DISK
809
920
DISK WITH A BCA
801

FIG. 2A

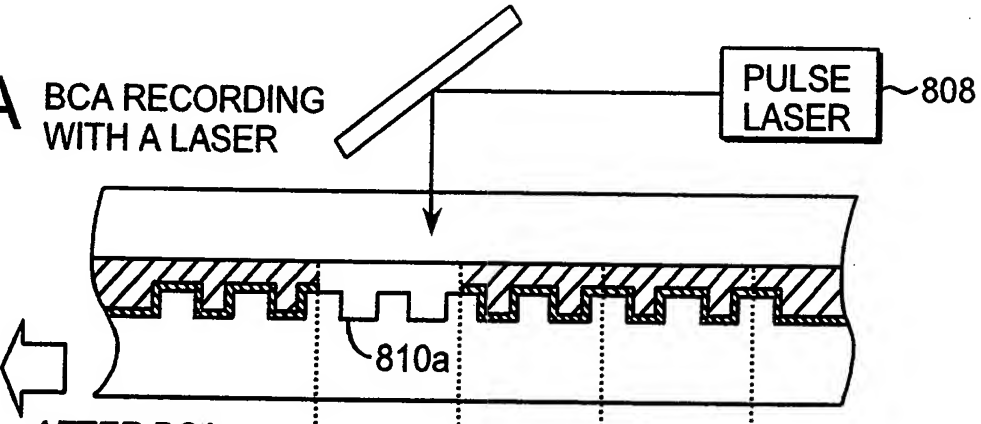


FIG. 2B

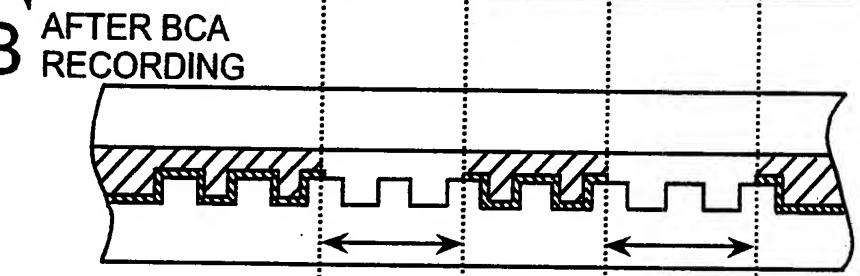


FIG. 2C

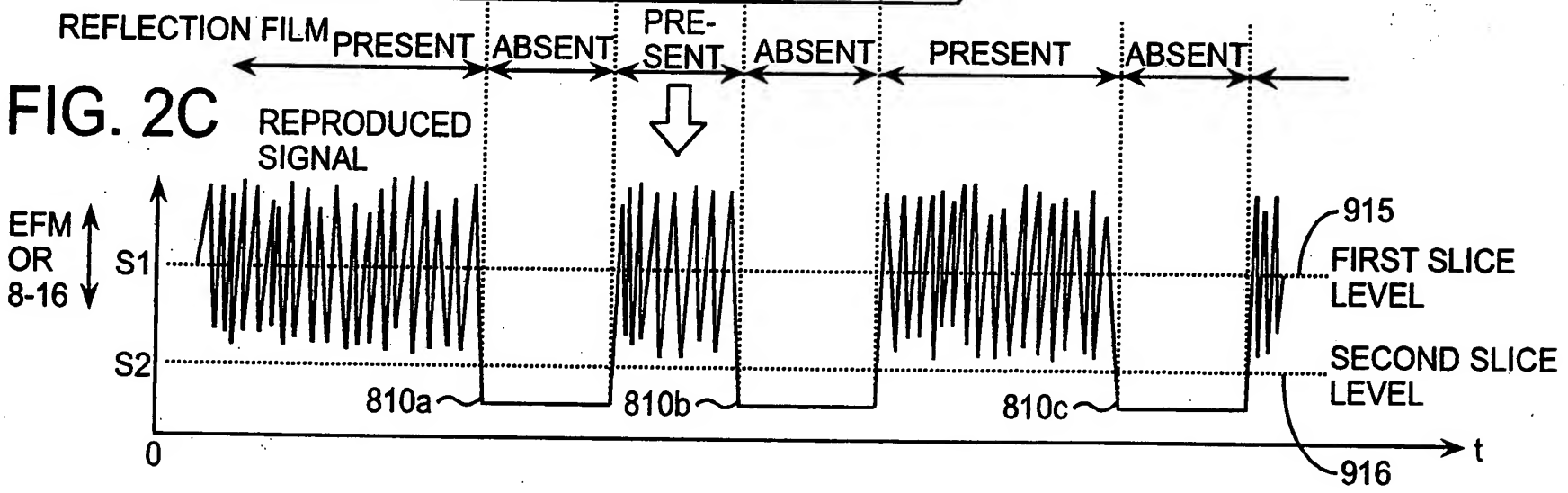


FIG. 3A

TOP PLAN

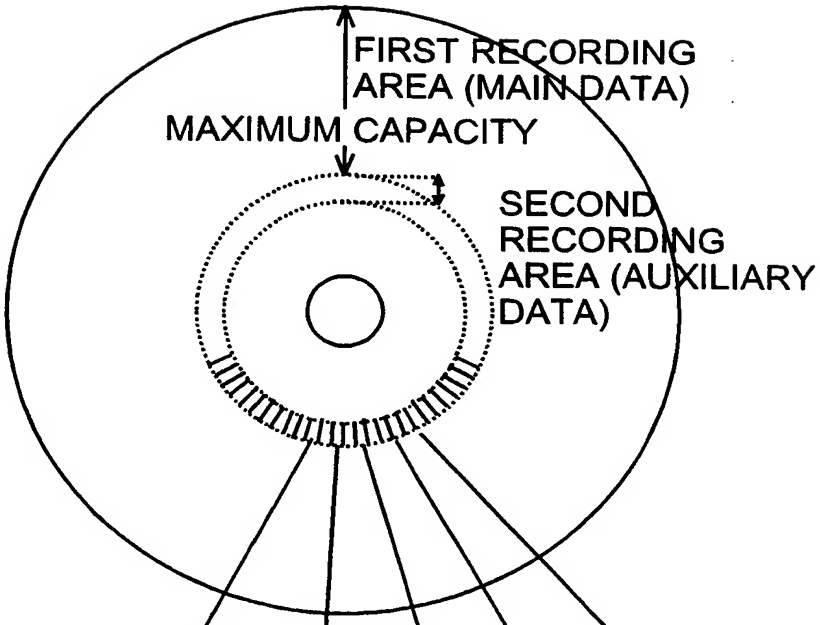


FIG. 3B BAR CODE PE MODULATION

RECORDED SIGNAL

FIG. 3C RECORDED SIGNAL

FIG. 3D RECORDED DATA

REPRODUCED SIGNAL

FIG. 3E REPRODUCED SIGNAL

FIG. 3F FILTERED

FIG. 3G REPRODUCED DATA

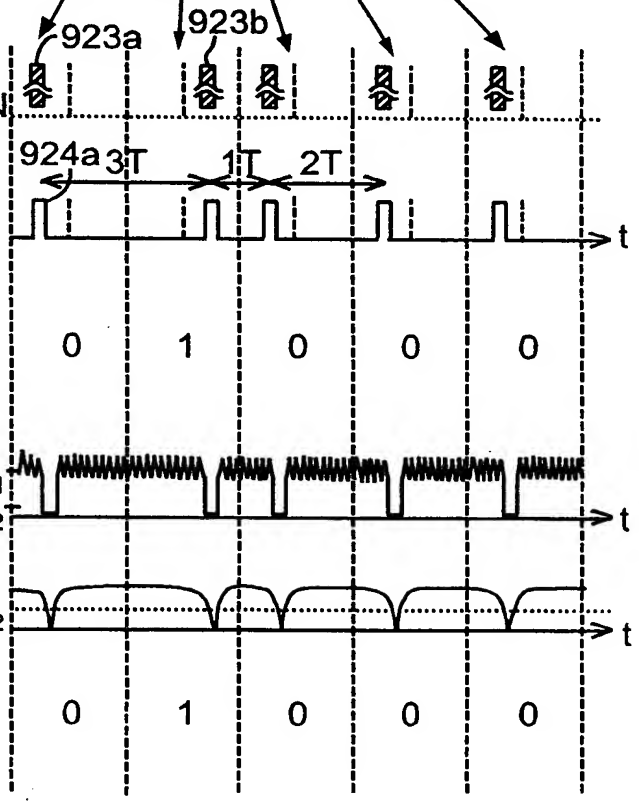


FIG. 4A

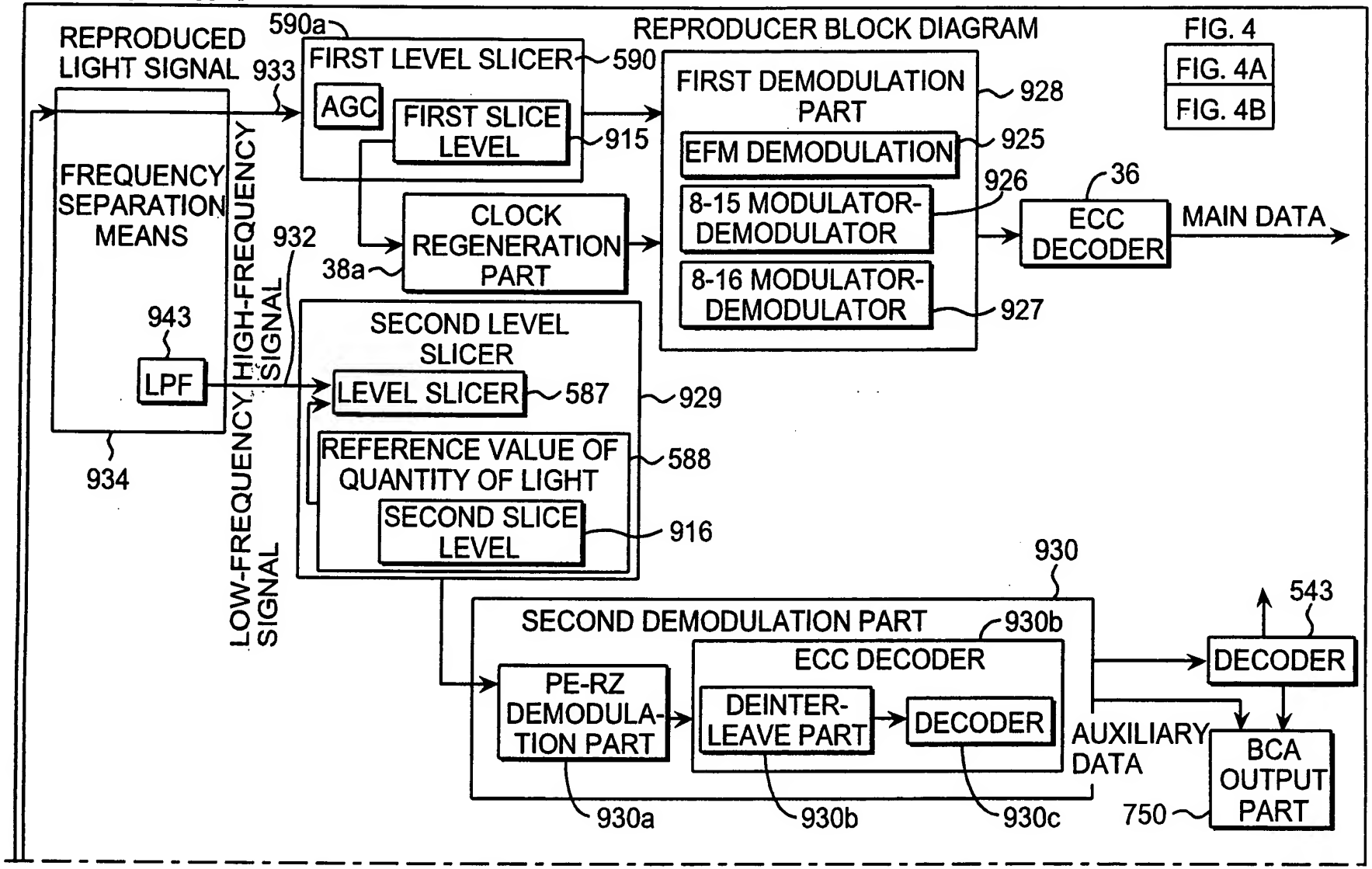

REPRODUCER BLOCK DIAGRAM
FIG. 4
FIG. 4A
FIG. 4B
REPRODUCED LIGHT SIGNAL
933
590a
FIRST LEVEL SLICER
590
AGC
FIRST SLICE LEVEL
915
FIRST DEMODULATION PART
928
EFM DEMODULATION
925
926
8-15 MODULATOR-DEMODULATOR
8-16 MODULATOR-DEMODULATOR
927
36
ECC DECODER
MAIN DATA
FREQUENCY SEPARATION MEANS
932
38a
CLOCK REGENERATION PART
943
LPF
HIGH-FREQUENCY SIGNAL
LOW-FREQUENCY SIGNAL
934
SECOND LEVEL SLICER
LEVEL SLICER
587
929
REFERENCE VALUE OF QUANTITY OF LIGHT
588
SECOND SLICE LEVEL
916
930
SECOND DEMODULATION PART
930b
ECC DECODER
PE-RZ DEMODULATION PART
DEINTER-LEAVE PART
DECODER
543
DECODER
AUXILIARY DATA
BCA OUTPUT PART
750
930a
930b
930c

FIG. 4B

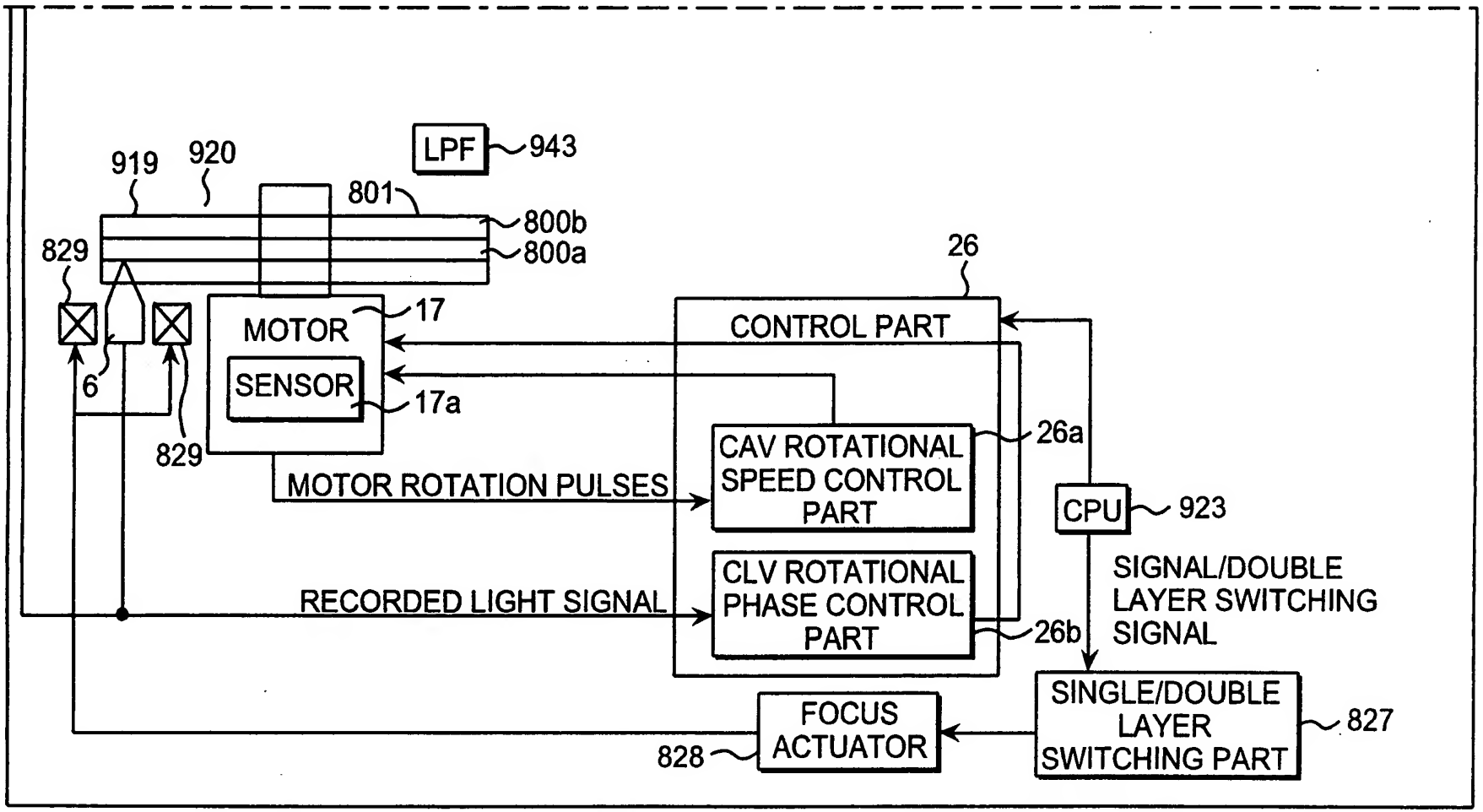
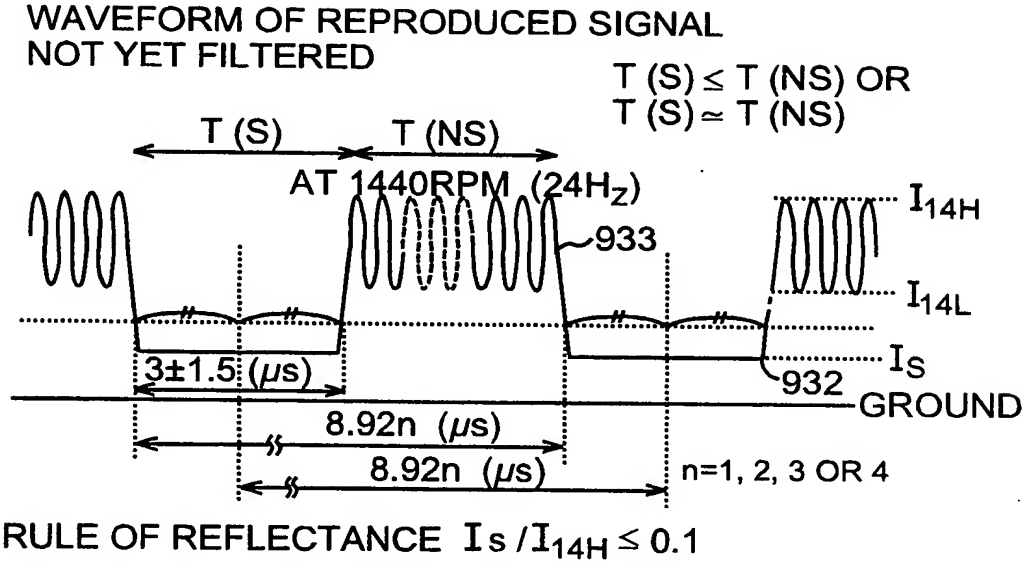

LPF
943
919
920
801
800b
800a
829
26
MOTOR
17
SENSOR
17a
6
829
CONTROL PART
CAV ROTATIONAL SPEED CONTROL PART
26a
MOTOR ROTATION PULSES
CPU
923
CLV ROTATIONAL PHASE CONTROL PART
RECORDED LIGHT SIGNAL
26b
SIGNAL/DOUBLE LAYER SWITCHING SIGNAL
SINGLE/DOUBLE LAYER SWITCHING PART
827
FOCUS ACTUATOR
828

FIG. 5A



RULE OF REFLECTANCE $I_S / I_{14H} \leq 0.1$

FIG. 5B SLIT DIMENSION ACCURACY (PRECISION)
(AT r=22.2mm)

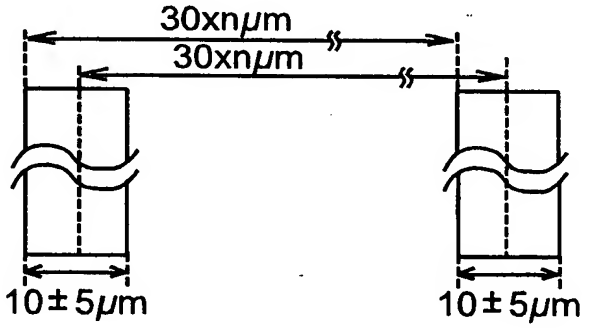


FIG. 6A

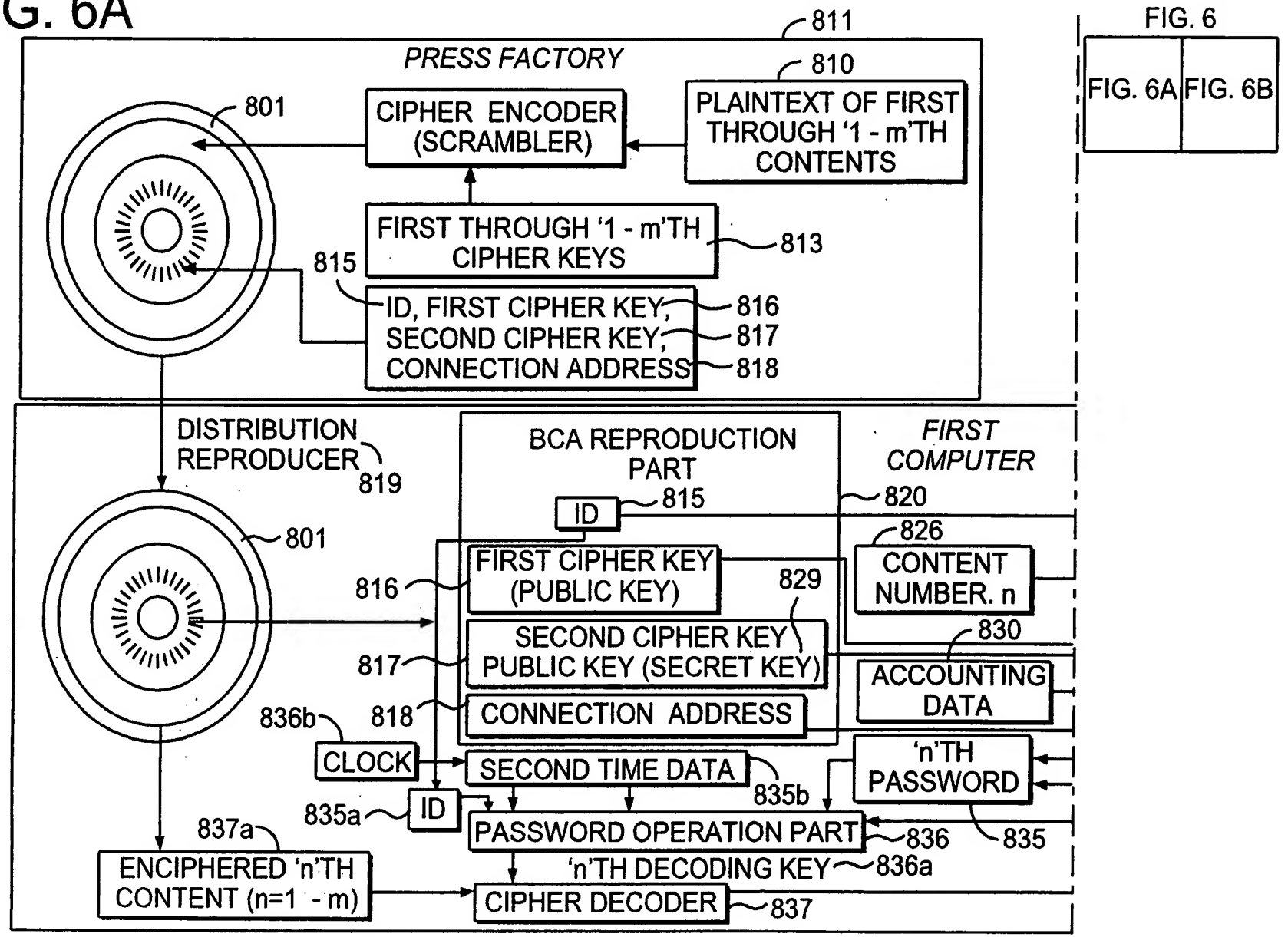


FIG. 6

FIG. 6A	FIG. 6B

FIG. 6B

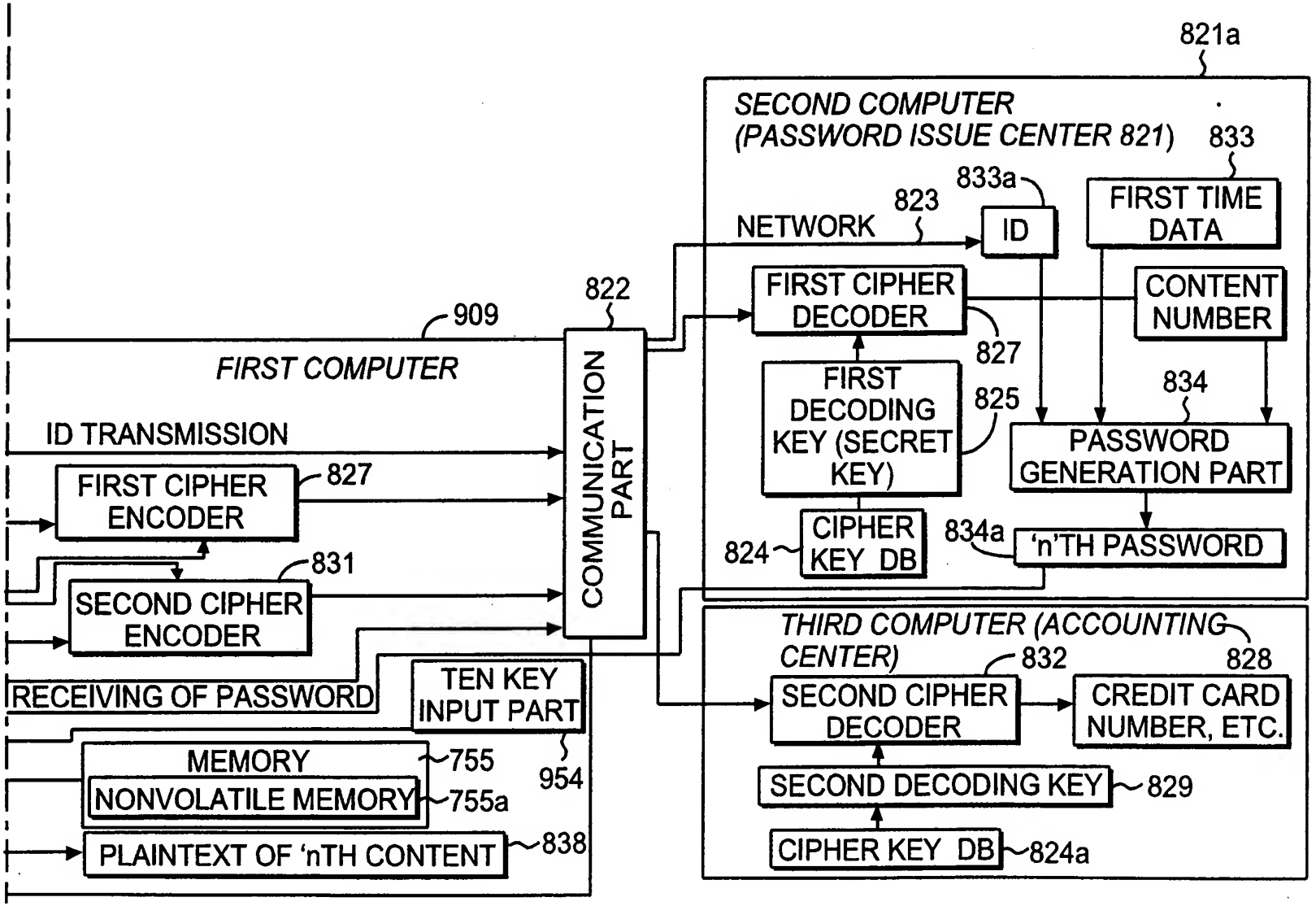

821a
SECOND COMPUTER
(PASSWORD ISSUE CENTER 821)
833
833a
823
NETWORK
ID
FIRST TIME DATA
FIRST CIPHER DECODER
CONTENT NUMBER
822
909
827
FIRST COMPUTER
FIRST DECODING KEY (SECRET KEY)
825
834
ID TRANSMISSION
PASSWORD GENERATION PART
COMMUNICATION PART
FIRST CIPHER ENCODER
827
CIPHER KEY DB
824
834a
'n'TH PASSWORD
831
SECOND CIPHER ENCODER
THIRD COMPUTER (ACCOUNTING CENTER)
832
828
RECEIVING OF PASSWORD
TEN KEY INPUT PART
SECOND CIPHER DECODER
CREDIT CARD NUMBER, ETC.
954
MEMORY
755
NONVOLATILE MEMORY
755a
SECOND DECODING KEY
829
PLAINTEXT OF 'nTH CONTENT
838
CIPHER KEY DB
824a

FIG. 7A

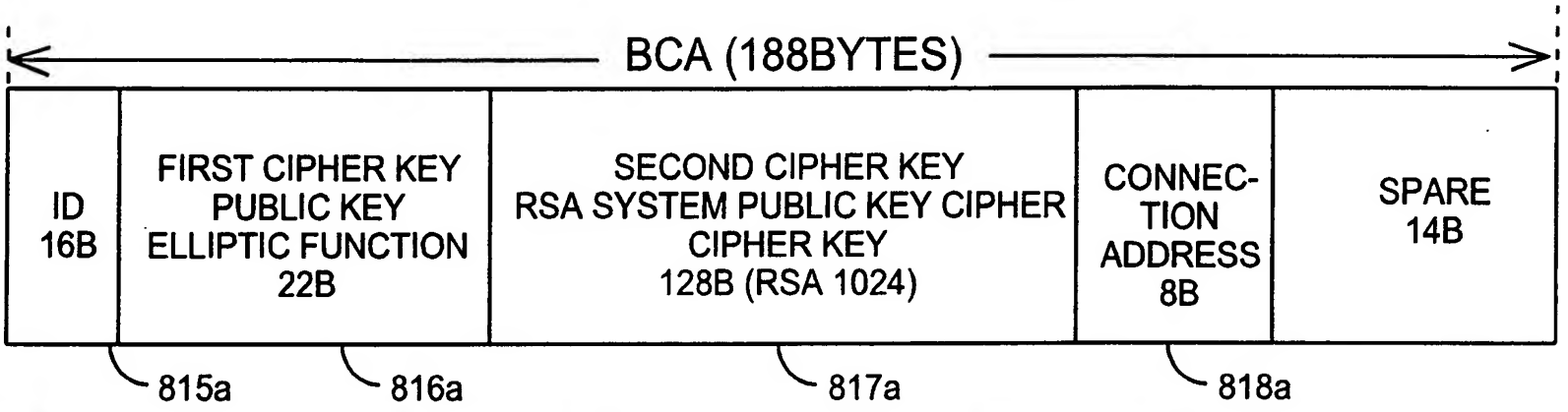


FIG. 7B

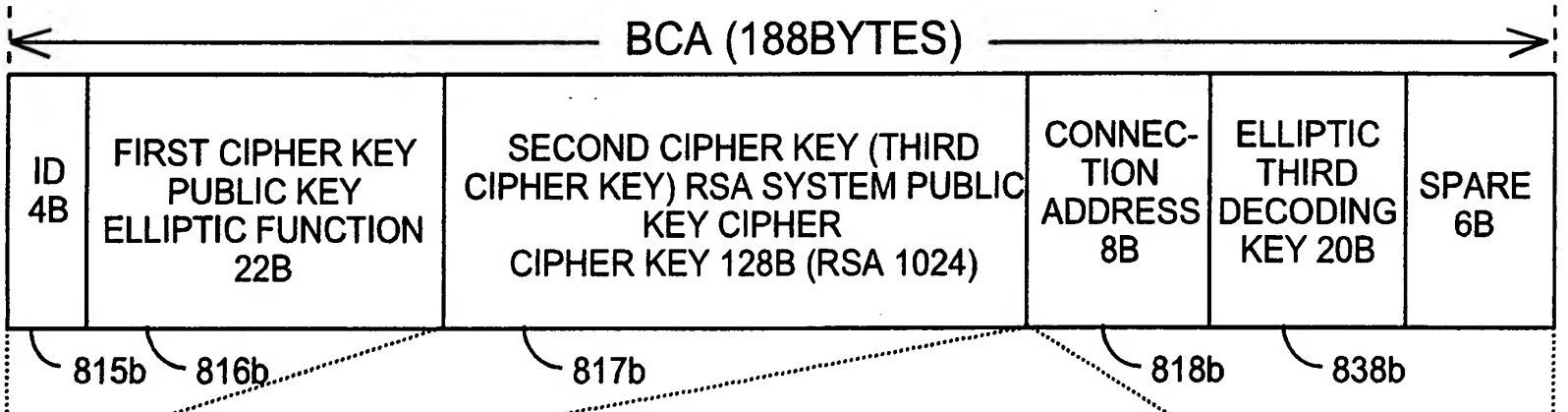


FIG. 7C

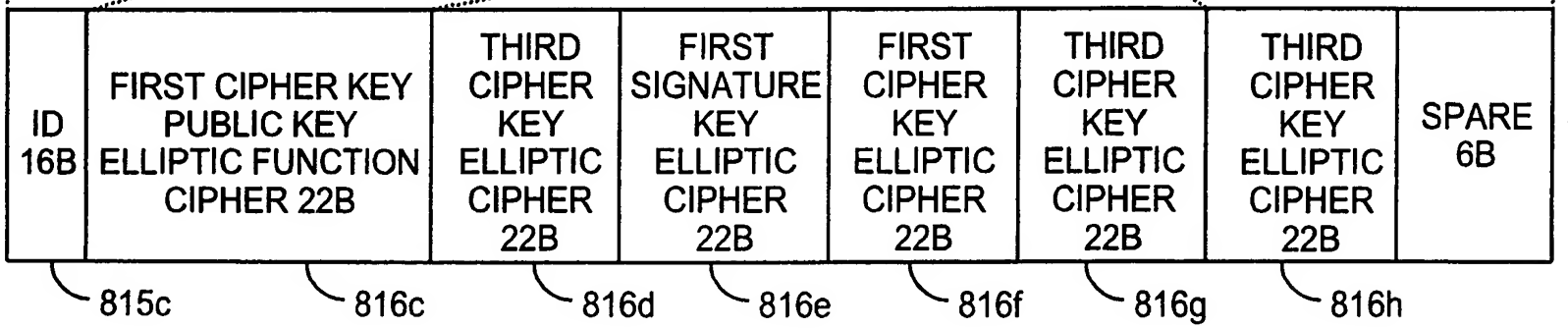


FIG 8A

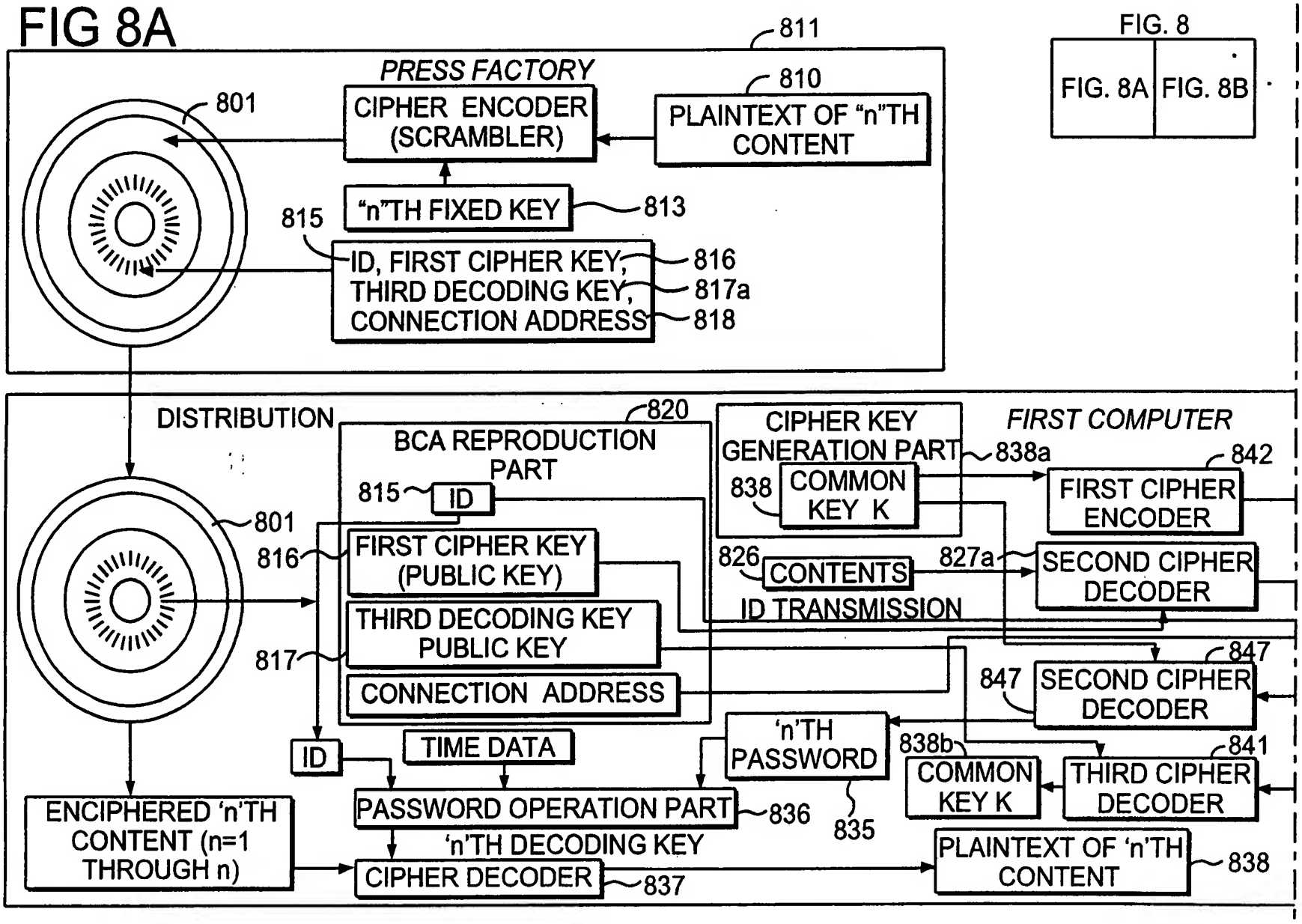


FIG. 8

FIG. 8A	FIG. 8B

FIG 8B

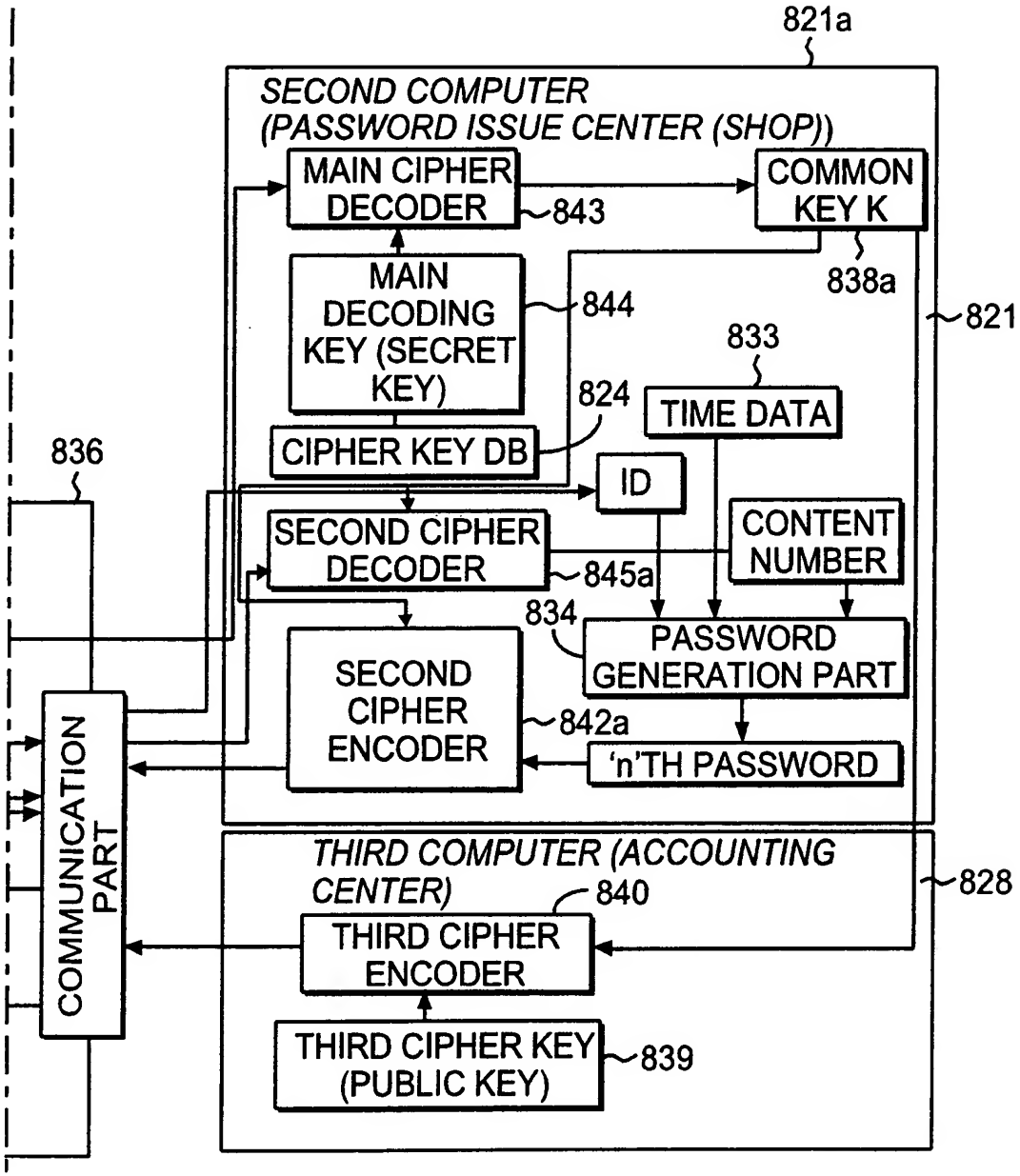

821a
SECOND COMPUTER
(PASSWORD ISSUE CENTER (SHOP))
MAIN CIPHER DECODER
843
COMMON KEY K
838a
821
MAIN DECODING KEY (SECRET KEY)
844
833
TIME DATA
824
CIPHER KEY DB
836
ID
SECOND CIPHER DECODER
845a
CONTENT NUMBER
834
PASSWORD GENERATION PART
SECOND CIPHER ENCODER
842a
'n'TH PASSWORD
COMMUNICATION PART
THIRD COMPUTER (ACCOUNTING CENTER)
840
828
THIRD CIPHER ENCODER
THIRD CIPHER KEY (PUBLIC KEY)
839

FIG. 9A

FIG. 9

FIG. 9A
FIG. 9B

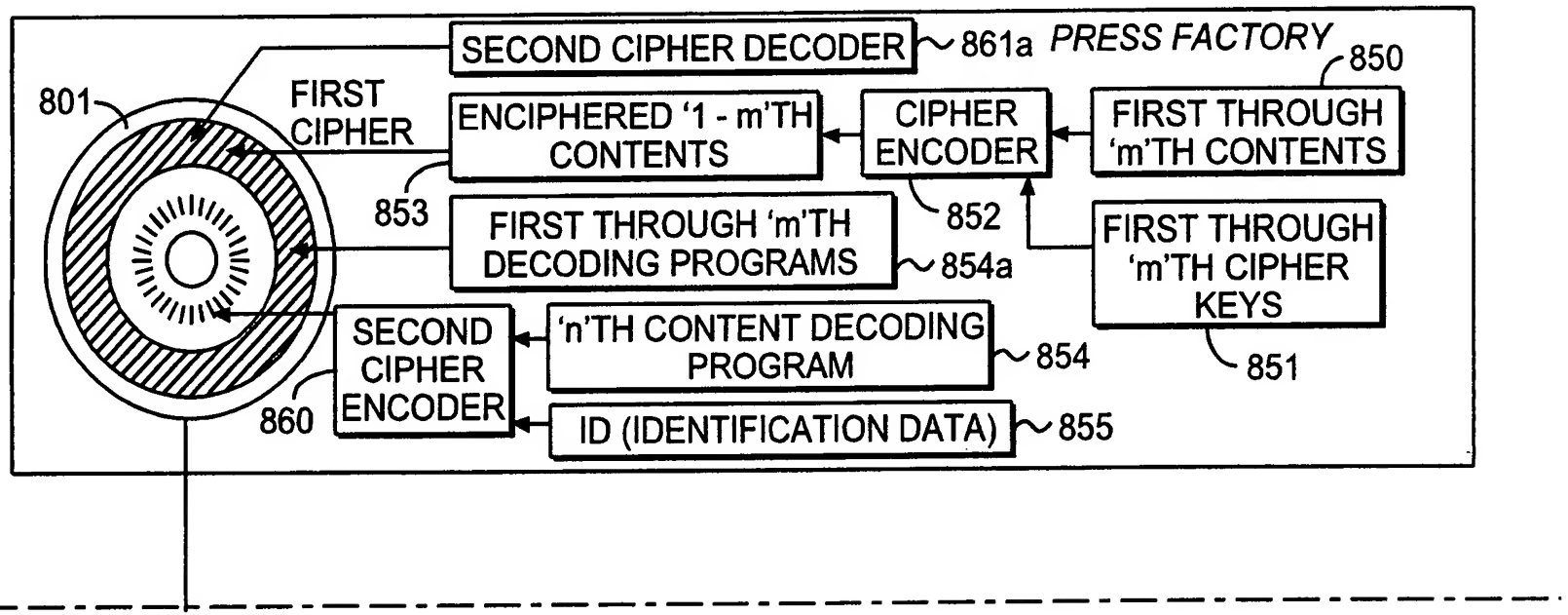


FIG. 9B

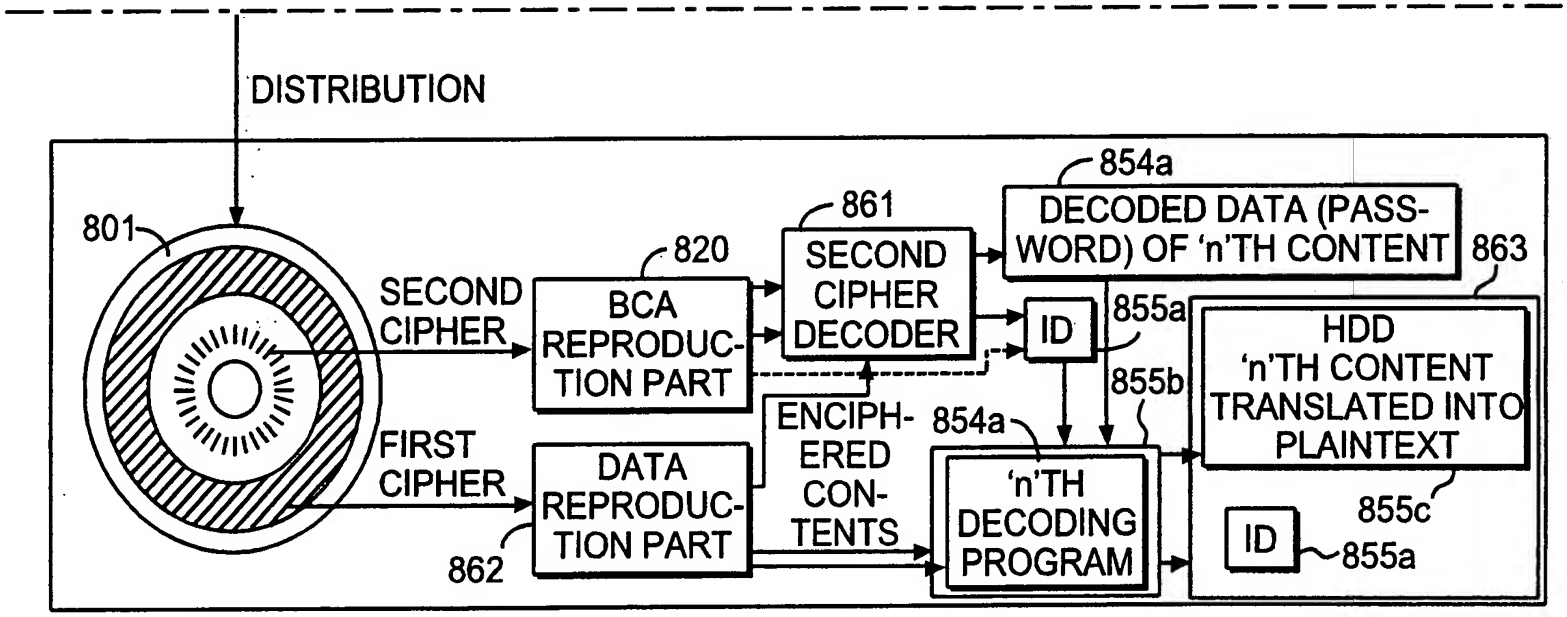

DISTRIBUTION
801
SECOND CIPHER
FIRST CIPHER
820
BCA REPRODUC-TION PART
DATA REPRODUC-TION PART
862
861
SECOND CIPHER DECODER
ENCIPH-ERED CON-TENTS
854a
DECODED DATA (PASS-WORD) OF 'n'TH CONTENT
863
ID
855a
855b
854a
'n'TH DECODING PROGRAM
HDD 'n'TH CONTENT TRANSLATED INTO PLAINTEXT
855c
ID
855a

FIG. 10

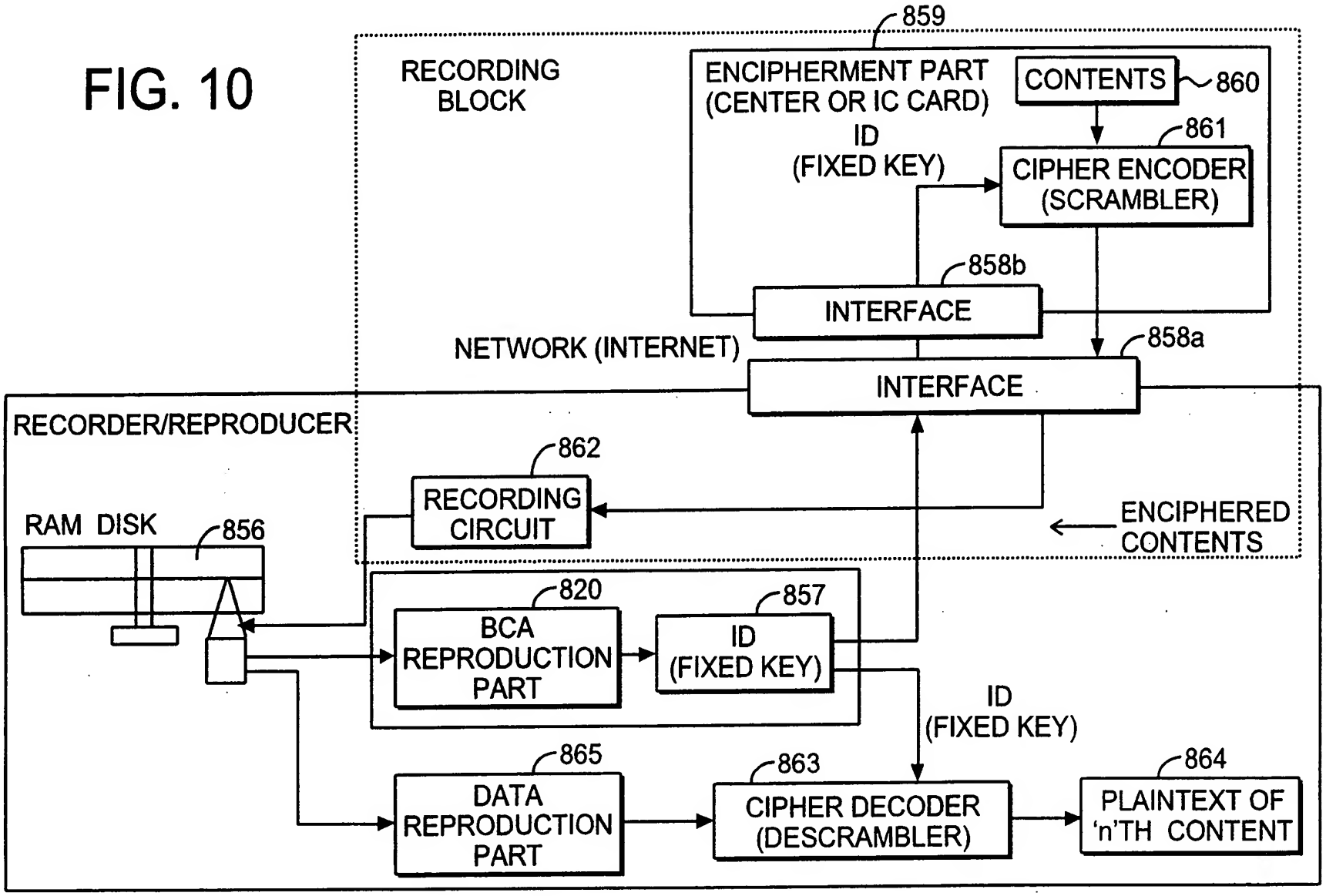

859
RECORDING BLOCK
ENCIPHERMENT PART (CENTER OR IC CARD)
CONTENTS
860
ID (FIXED KEY)
861
CIPHER ENCODER (SCRAMBLER)
858b
INTERFACE
NETWORK (INTERNET)
858a
INTERFACE
RECORDER/REPRODUCER
862
RECORDING CIRCUIT
ENCIPHERED CONTENTS
RAM DISK
856
820
BCA REPRODUCTION PART
857
ID (FIXED KEY)
ID (FIXED KEY)
865
DATA REPRODUCTION PART
863
CIPHER DECODER (DESCRAMBLER)
864
PLAINTEXT OF 'n'TH CONTENT

FIG. 11

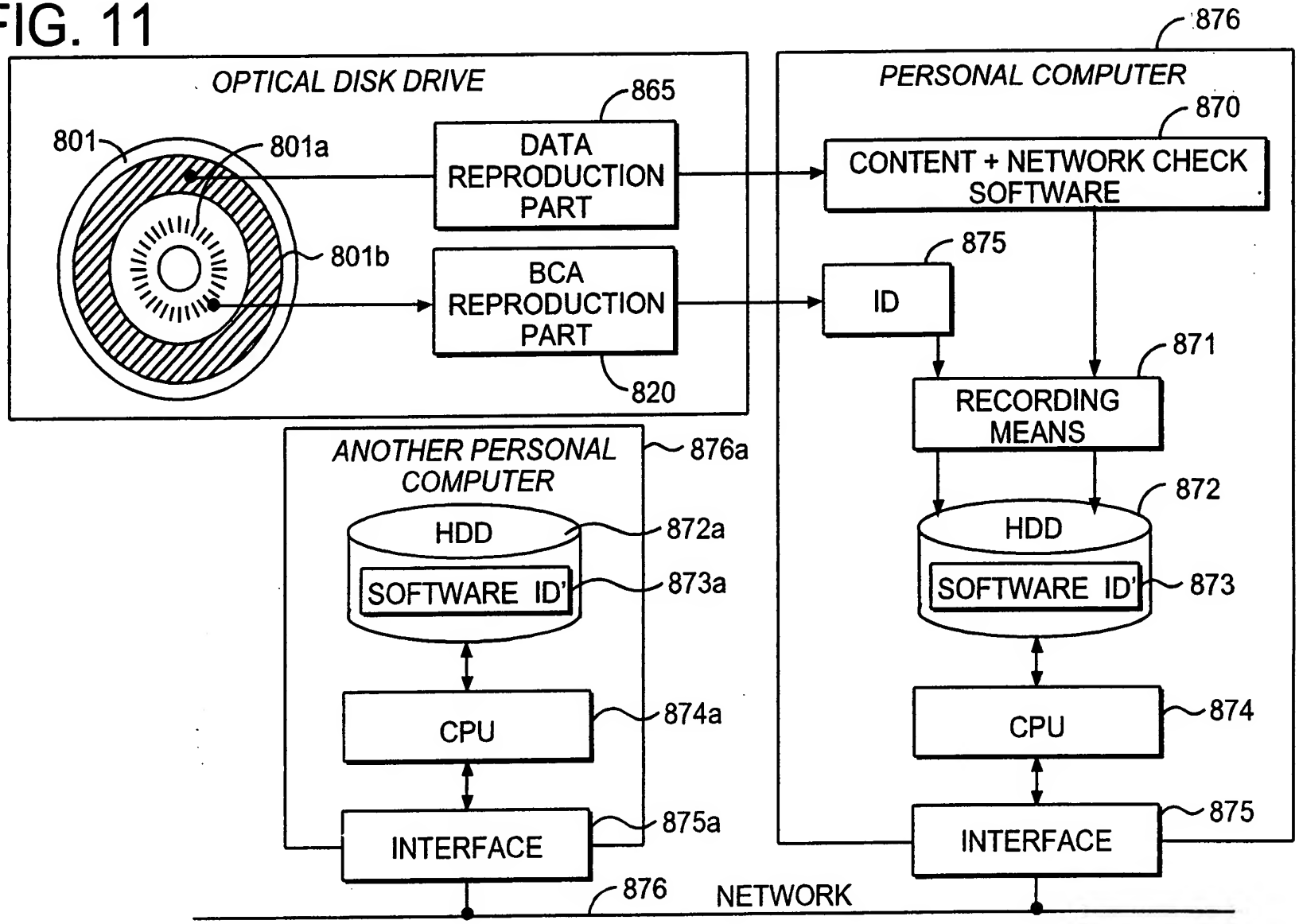

OPTICAL DISK DRIVE
801
801a
801b
DATA REPRODUCTION PART
865
BCA REPRODUCTION PART
820
PERSONAL COMPUTER
876
CONTENT + NETWORK CHECK SOFTWARE
870
ID
875
RECORDING MEANS
871
HDD
872
SOFTWARE ID'
873
CPU
874
INTERFACE
875
ANOTHER PERSONAL COMPUTER
876a
HDD
872a
SOFTWARE ID'
873a
CPU
874a
INTERFACE
875a
876
NETWORK

FIG. 12

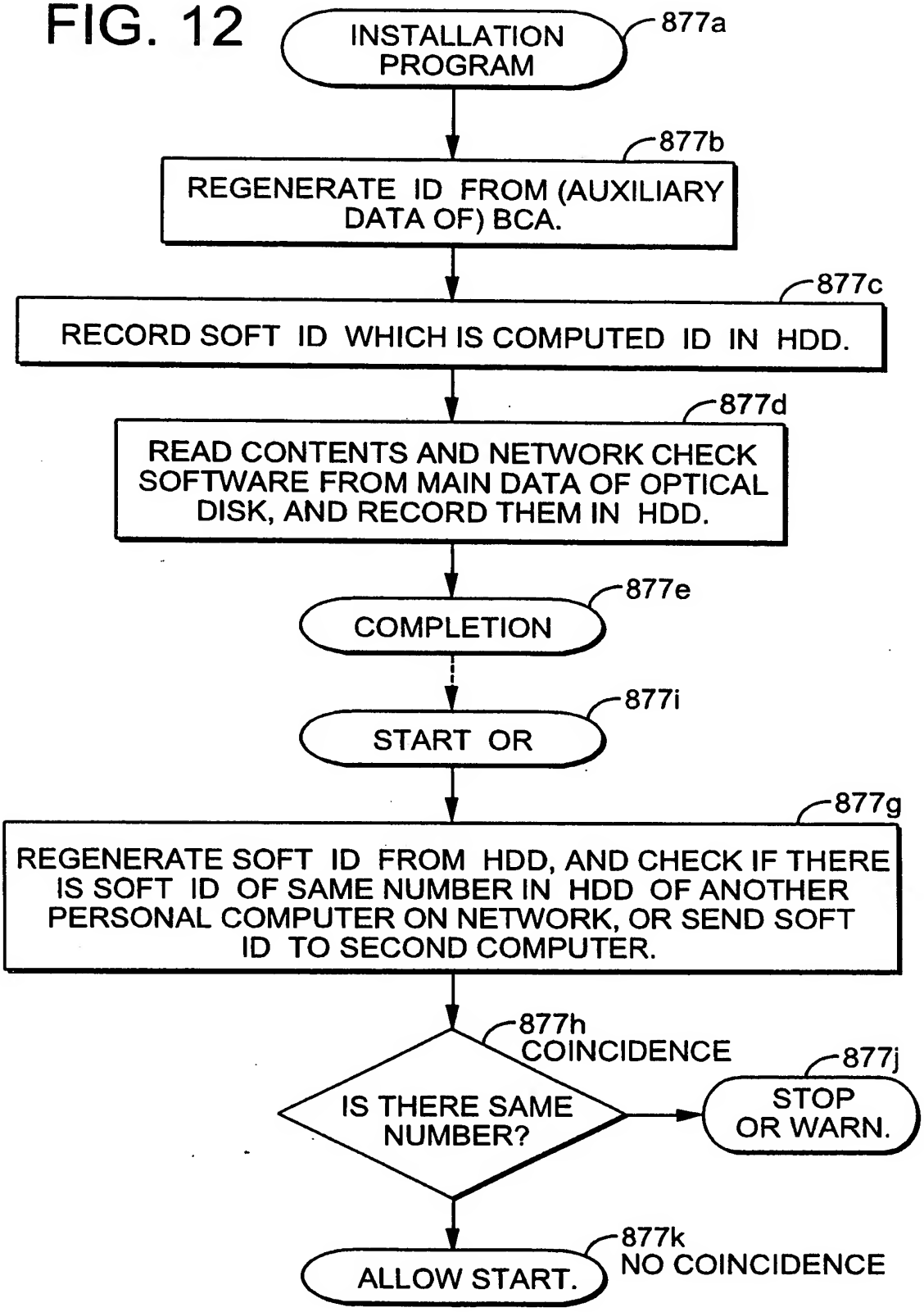

INSTALLATION PROGRAM
877a
877b
REGENERATE ID FROM (AUXILIARY DATA OF) BCA.
877c
RECORD SOFT ID WHICH IS COMPUTED ID IN HDD.
877d
READ CONTENTS AND NETWORK CHECK SOFTWARE FROM MAIN DATA OF OPTICAL DISK, AND RECORD THEM IN HDD.
877e
COMPLETION
877i
START OR
877g
REGENERATE SOFT ID FROM HDD, AND CHECK IF THERE IS SOFT ID OF SAME NUMBER IN HDD OF ANOTHER PERSONAL COMPUTER ON NETWORK, OR SEND SOFT ID TO SECOND COMPUTER.
877h
COINCIDENCE
IS THERE SAME NUMBER?
877j
STOP OR WARN.
877k
NO COINCIDENCE
ALLOW START.

FIG. 13A

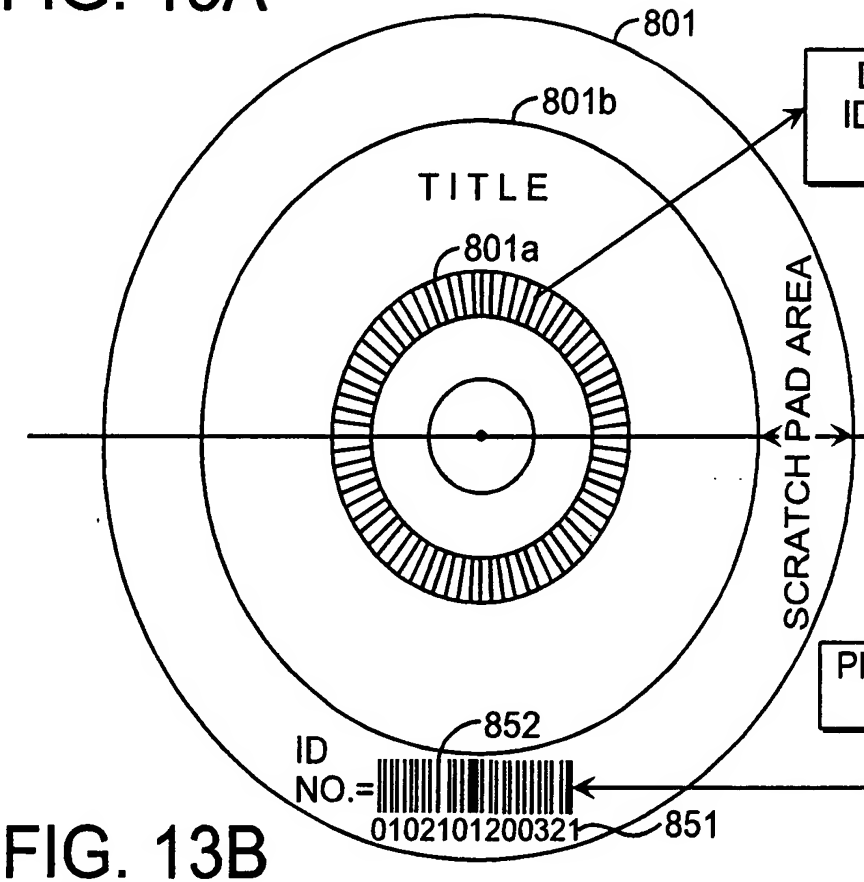
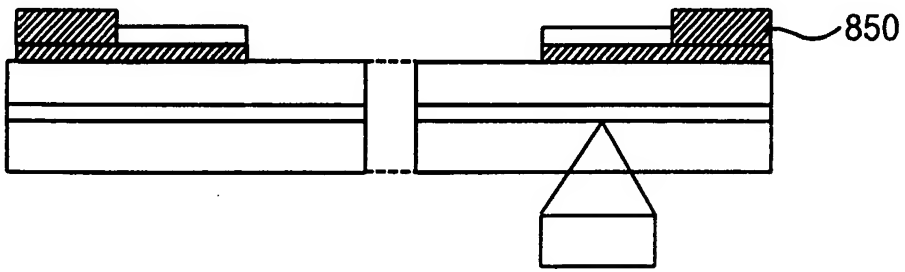


FIG. 13B



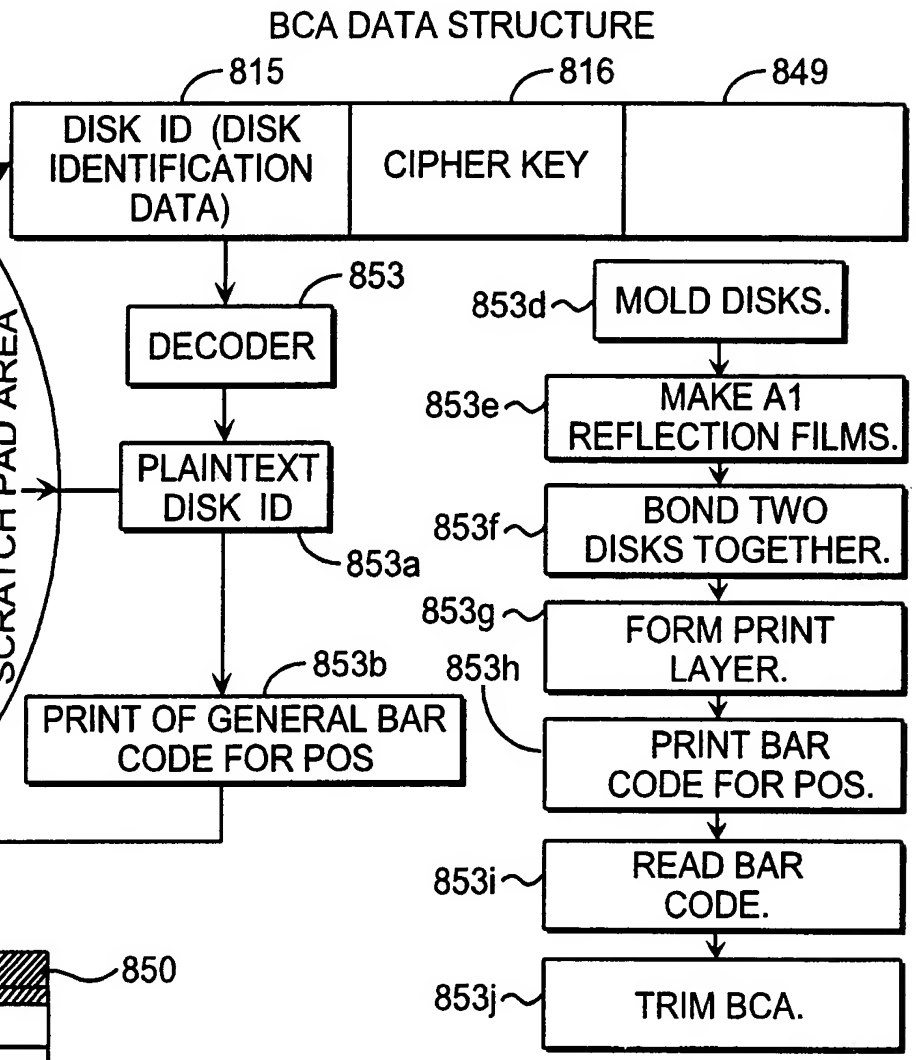


FIG. 13C

FIG. 14A

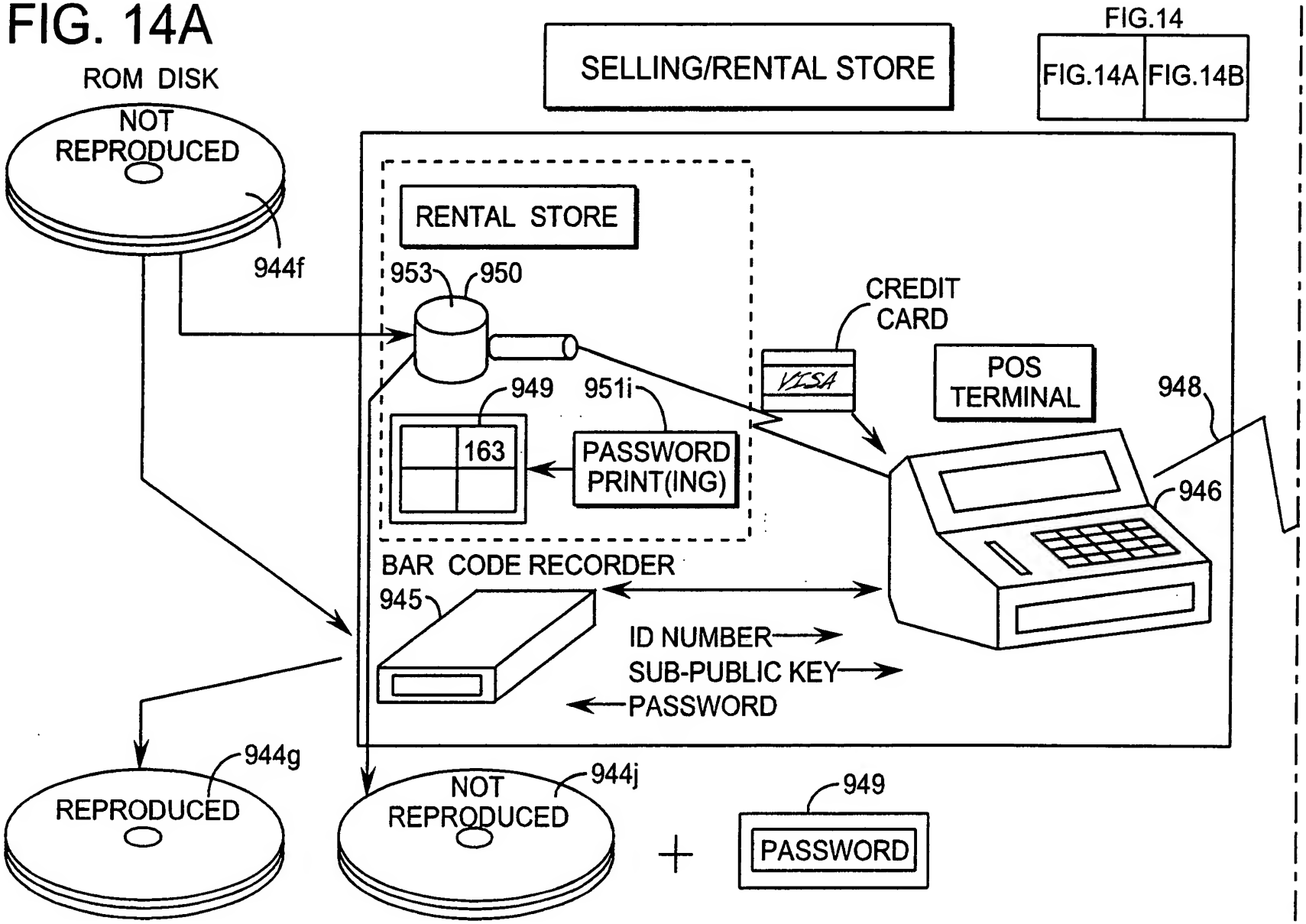


FIG.14
FIG.14A
FIG.14B
SELLING/RENTAL STORE
ROM DISK
NOT REPRODUCED
944f
RENTAL STORE
953
950
CREDIT CARD
VISA
POS TERMINAL
948
949
951i
163
PASSWORD PRINT(ING)
946
BAR CODE RECORDER
945
ID NUMBER
SUB-PUBLIC KEY
PASSWORD
944g
REPRODUCED
NOT REPRODUCED
944j
949
PASSWORD

FIG. 14B

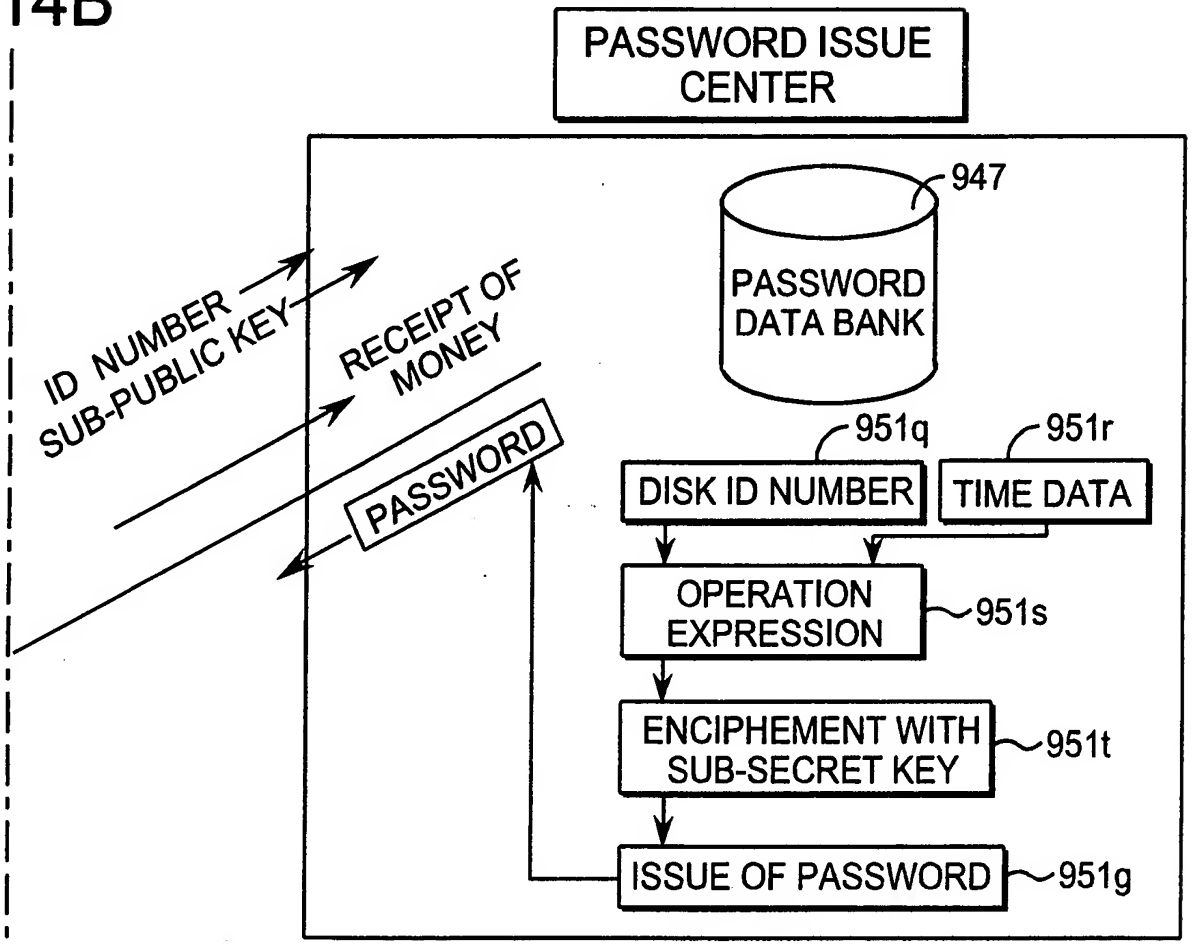

PASSWORD ISSUE CENTER
947
PASSWORD DATA BANK
ID NUMBER
SUB-PUBLIC KEY
RECEIPT OF MONEY
PASSWORD
951q
951r
DISK ID NUMBER
TIME DATA
OPERATION EXPRESSION
951s
ENCIPHEMENT WITH SUB-SECRET KEY
951t
ISSUE OF PASSWORD
951g

FIG. 15A

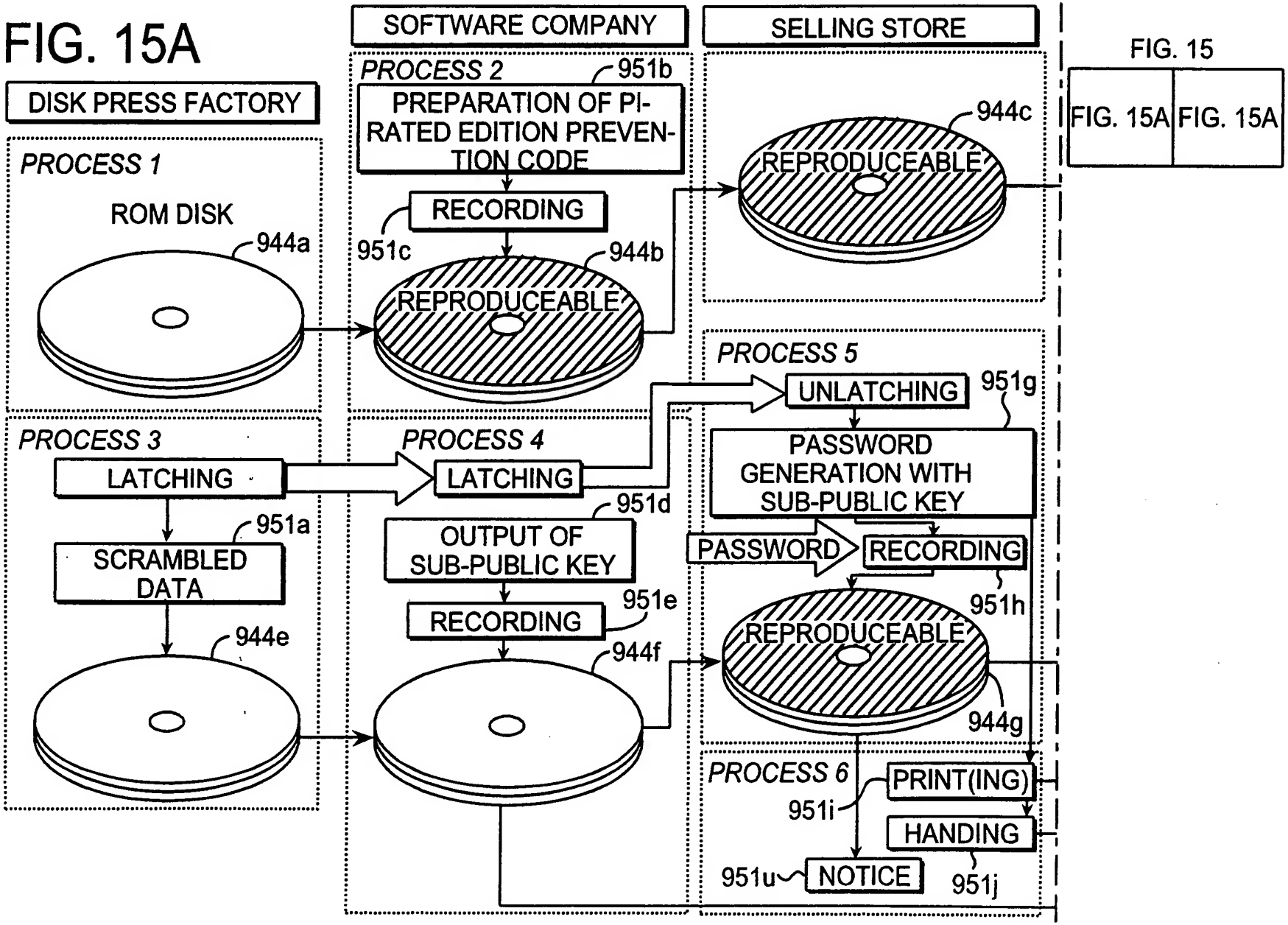


FIG. 15

FIG. 15A	FIG. 15A

FIG. 15B

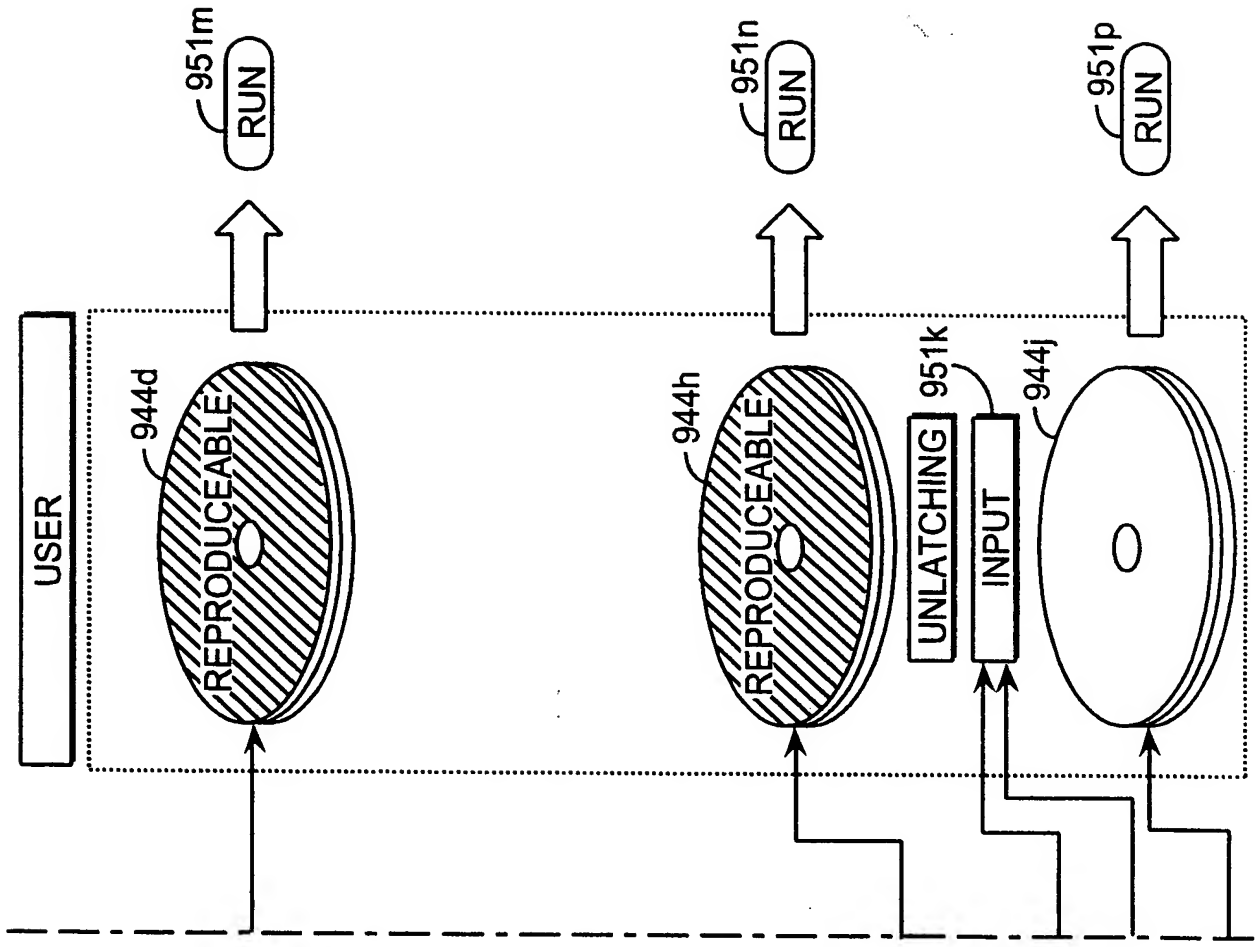

USER
951m
RUN
944d
REPRODUCEABLE
951n
RUN
944h
REPRODUCEABLE
951k
UNLATCHING
INPUT
944j
951p
RUN

FIG. 16

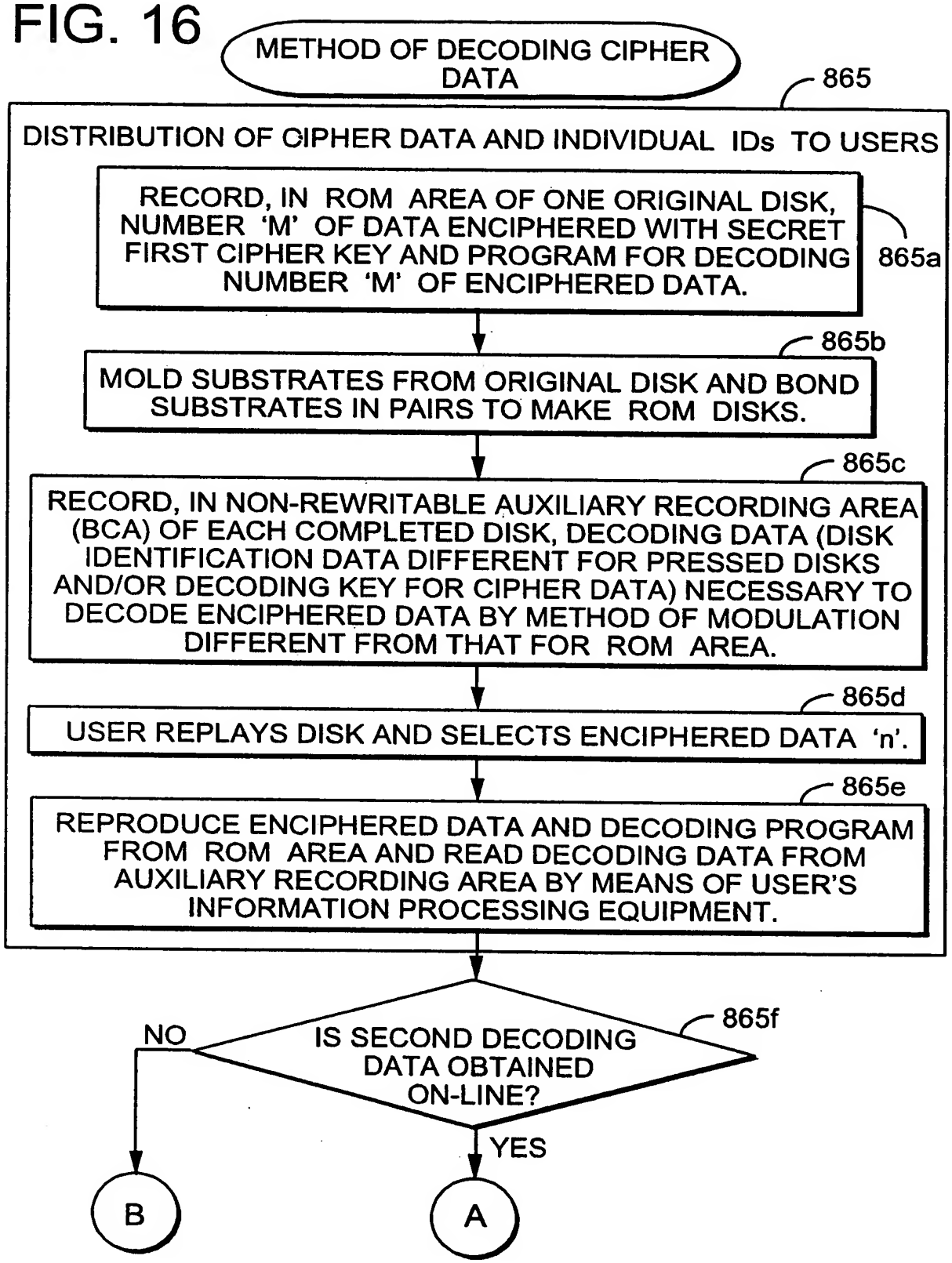

METHOD OF DECODING CIPHER DATA
865
DISTRIBUTION OF CIPHER DATA AND INDIVIDUAL IDs TO USERS
RECORD, IN ROM AREA OF ONE ORIGINAL DISK, NUMBER 'M' OF DATA ENCIPHERED WITH SECRET FIRST CIPHER KEY AND PROGRAM FOR DECODING NUMBER 'M' OF ENCIPHERED DATA.
865a
865b
MOLD SUBSTRATES FROM ORIGINAL DISK AND BOND SUBSTRATES IN PAIRS TO MAKE ROM DISKS.
865c
RECORD, IN NON-REWRITABLE AUXILIARY RECORDING AREA (BCA) OF EACH COMPLETED DISK, DECODING DATA (DISK IDENTIFICATION DATA DIFFERENT FOR PRESSED DISKS AND/OR DECODING KEY FOR CIPHER DATA) NECESSARY TO DECODE ENCIPHERED DATA BY METHOD OF MODULATION DIFFERENT FROM THAT FOR ROM AREA.
865d
USER REPLAYS DISK AND SELECTS ENCIPHERED DATA 'n'.
865e
REPRODUCE ENCIPHERED DATA AND DECODING PROGRAM FROM ROM AREA AND READ DECODING DATA FROM AUXILIARY RECORDING AREA BY MEANS OF USER'S INFORMATION PROCESSING EQUIPMENT.
865f
IS SECOND DECODING DATA OBTAINED ON-LINE?
NO
YES
B
A

FIG. 17

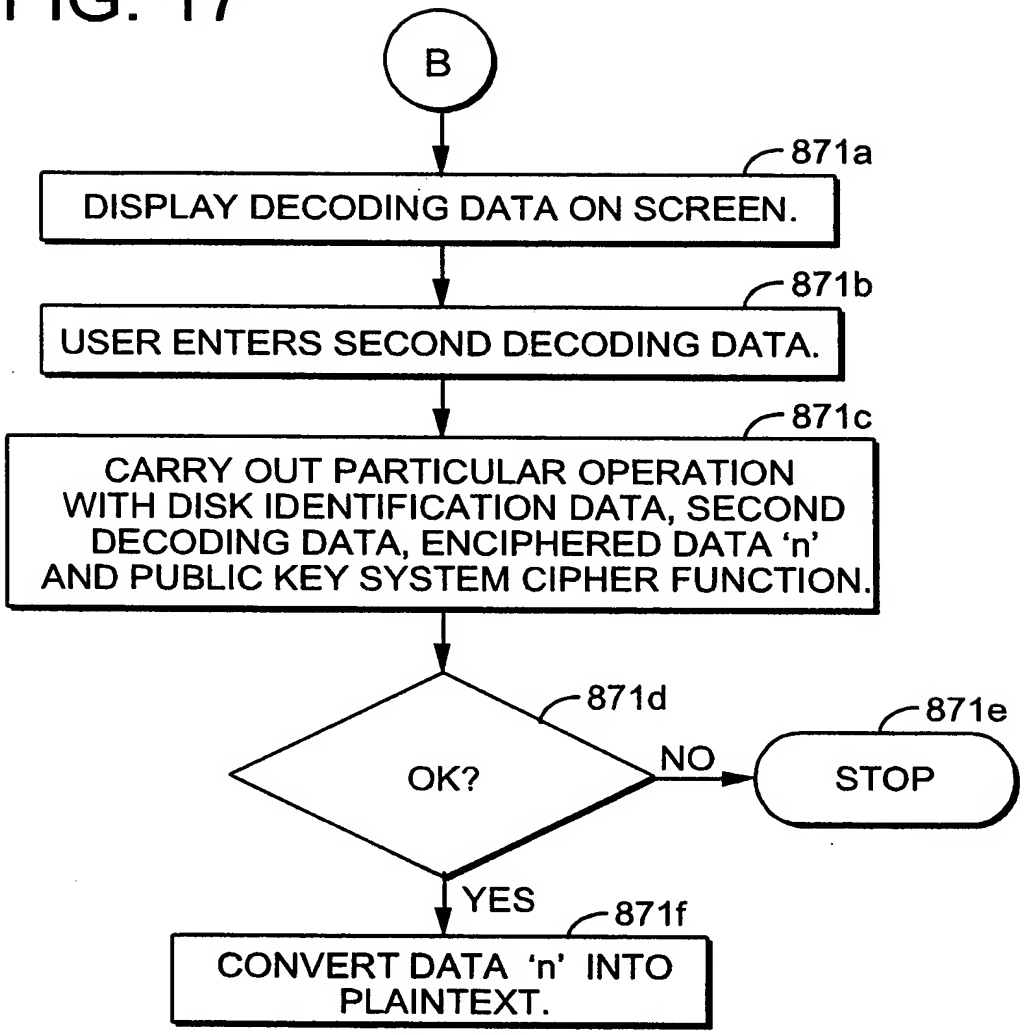

B
871a
DISPLAY DECODING DATA ON SCREEN.
871b
USER ENTERS SECOND DECODING DATA.
871c
CARRY OUT PARTICULAR OPERATION WITH DISK IDENTIFICATION DATA, SECOND DECODING DATA, ENCIPHERED DATA 'n' AND PUBLIC KEY SYSTEM CIPHER FUNCTION.
871d
OK?
NO
871e
STOP
YES
871f
CONVERT DATA 'n' INTO PLAINTEXT.

FIG. 18

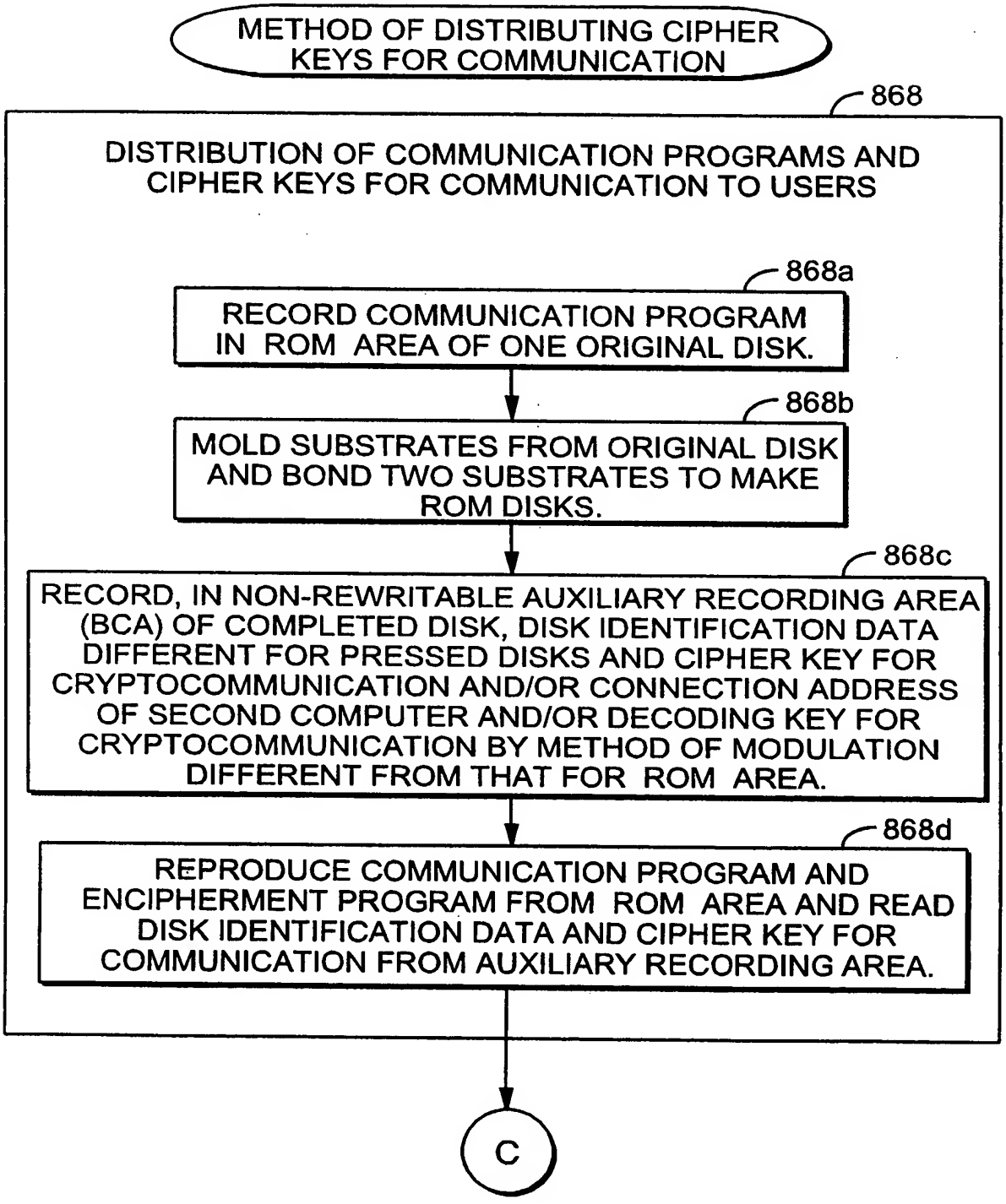

METHOD OF DISTRIBUTING CIPHER KEYS FOR COMMUNICATION
868
DISTRIBUTION OF COMMUNICATION PROGRAMS AND CIPHER KEYS FOR COMMUNICATION TO USERS
868a
RECORD COMMUNICATION PROGRAM IN ROM AREA OF ONE ORIGINAL DISK.
868b
MOLD SUBSTRATES FROM ORIGINAL DISK AND BOND TWO SUBSTRATES TO MAKE ROM DISKS.
868c
RECORD, IN NON-REWRITABLE AUXILIARY RECORDING AREA (BCA) OF COMPLETED DISK, DISK IDENTIFICATION DATA DIFFERENT FOR PRESSED DISKS AND CIPHER KEY FOR CRYPTOCOMMUNICATION AND/OR CONNECTION ADDRESS OF SECOND COMPUTER AND/OR DECODING KEY FOR CRYPTOCOMMUNICATION BY METHOD OF MODULATION DIFFERENT FROM THAT FOR ROM AREA.
868d
REPRODUCE COMMUNICATION PROGRAM AND ENCIPHERMENT PROGRAM FROM ROM AREA AND READ DISK IDENTIFICATION DATA AND CIPHER KEY FOR COMMUNICATION FROM AUXILIARY RECORDING AREA.
C

FIG. 19

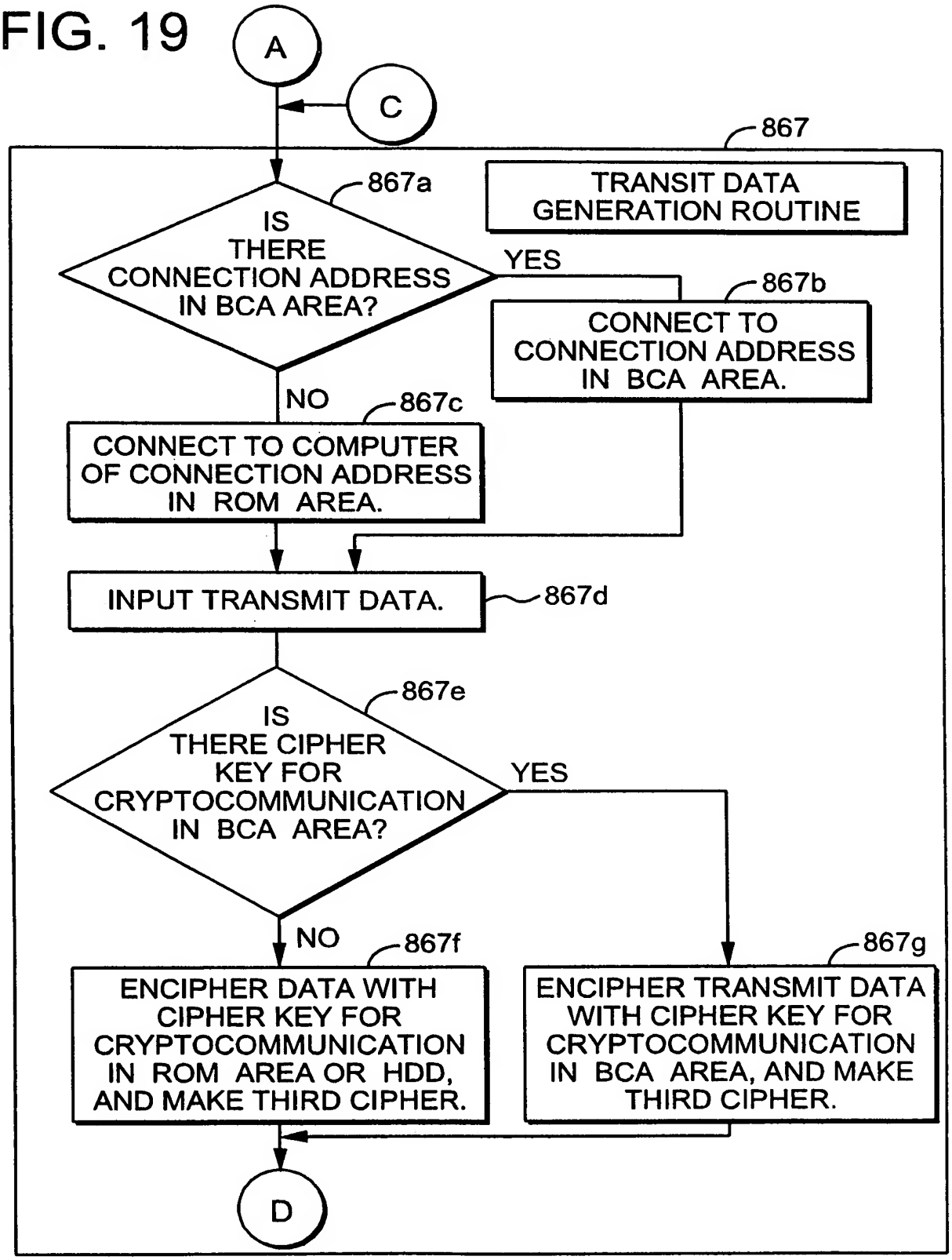

A
C
867
867a
IS THERE CONNECTION ADDRESS IN BCA AREA?
TRANSIT DATA GENERATION ROUTINE
YES
867b
CONNECT TO CONNECTION ADDRESS IN BCA AREA.
NO
867c
CONNECT TO COMPUTER OF CONNECTION ADDRESS IN ROM AREA.
INPUT TRANSMIT DATA.
867d
867e
IS THERE CIPHER KEY FOR CRYPTOCOMMUNICATION IN BCA AREA?
YES
NO
867f
ENCIPHER DATA WITH CIPHER KEY FOR CRYPTOCOMMUNICATION IN ROM AREA OR HDD, AND MAKE THIRD CIPHER.
867g
ENCIPHER TRANSMIT DATA WITH CIPHER KEY FOR CRYPTOCOMMUNICATION IN BCA AREA, AND MAKE THIRD CIPHER.
D

FIG. 20A

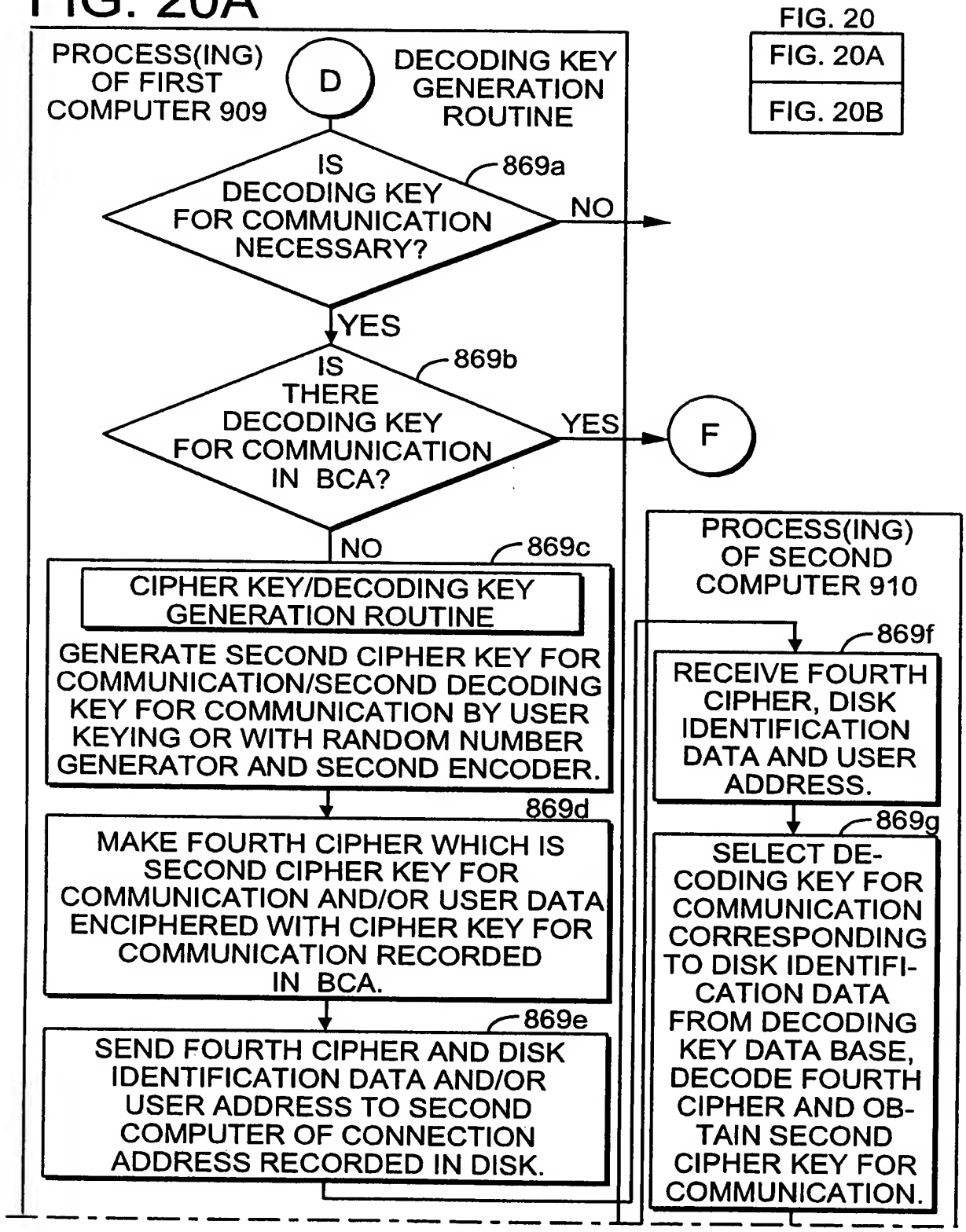


FIG. 20

FIG. 20A
FIG. 20B

FIG. 20B

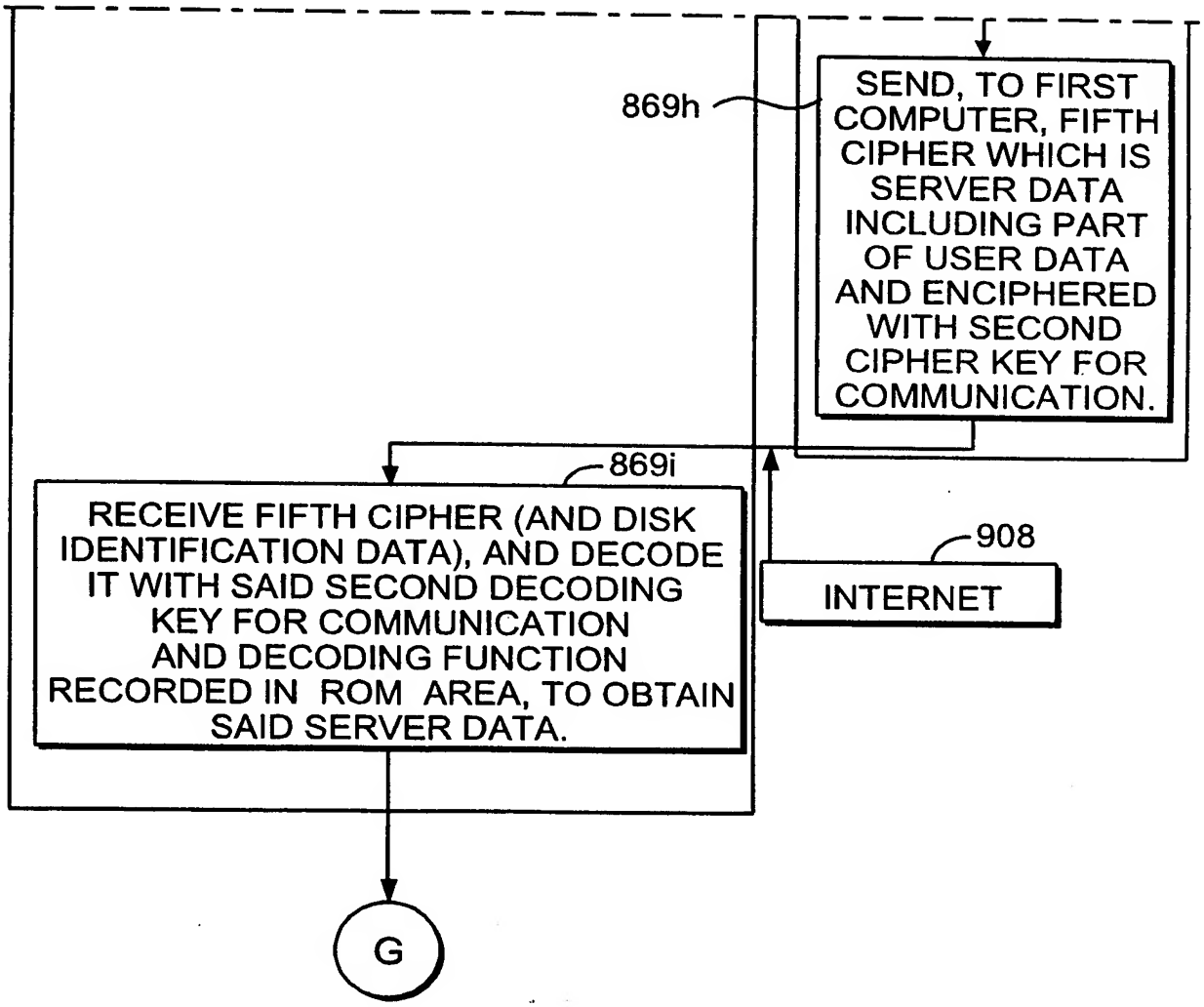

869h
SEND, TO FIRST COMPUTER, FIFTH CIPHER WHICH IS SERVER DATA INCLUDING PART OF USER DATA AND ENCIPHERED WITH SECOND CIPHER KEY FOR COMMUNICATION.
869i
RECEIVE FIFTH CIPHER (AND DISK IDENTIFICATION DATA), AND DECODE IT WITH SAID SECOND DECODING KEY FOR COMMUNICATION AND DECODING FUNCTION RECORDED IN ROM AREA, TO OBTAIN SAID SERVER DATA.
908
INTERNET
G

FIG. 21A

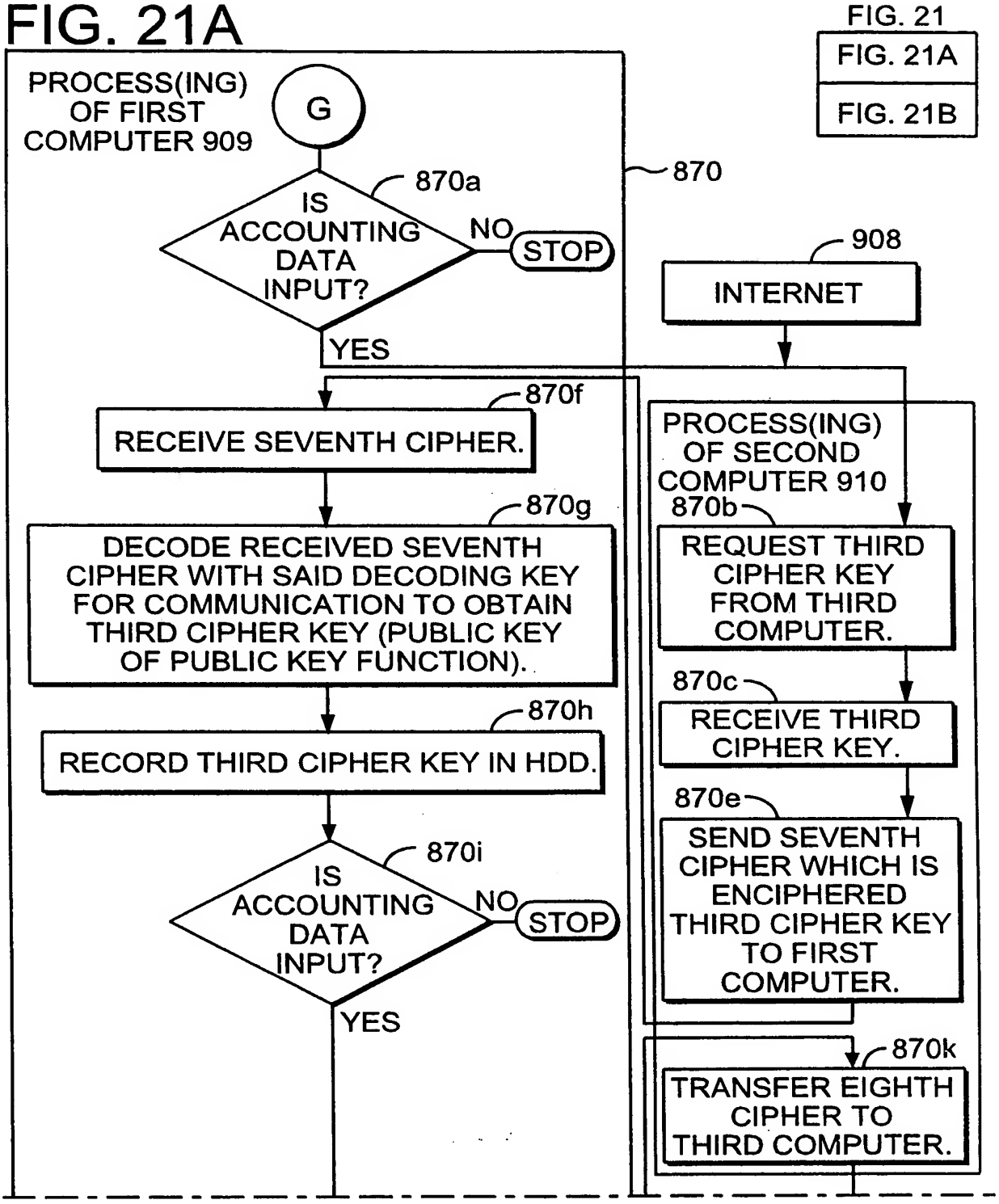


FIG. 21
FIG. 21A
FIG. 21B
PROCESS(ING) OF FIRST COMPUTER 909
G
870
870a
IS ACCOUNTING DATA INPUT?
NO
STOP
YES
908
INTERNET
870f
RECEIVE SEVENTH CIPHER.
PROCESS(ING) OF SECOND COMPUTER 910
870b
REQUEST THIRD CIPHER KEY FROM THIRD COMPUTER.
870g
DECODE RECEIVED SEVENTH CIPHER WITH SAID DECODING KEY FOR COMMUNICATION TO OBTAIN THIRD CIPHER KEY (PUBLIC KEY OF PUBLIC KEY FUNCTION).
870c
RECEIVE THIRD CIPHER KEY.
870h
RECORD THIRD CIPHER KEY IN HDD.
870e
SEND SEVENTH CIPHER WHICH IS ENCIPHERED THIRD CIPHER KEY TO FIRST COMPUTER.
870i
IS ACCOUNTING DATA INPUT?
NO
STOP
YES
870k
TRANSFER EIGHTH CIPHER TO THIRD COMPUTER.

FIG. 21B

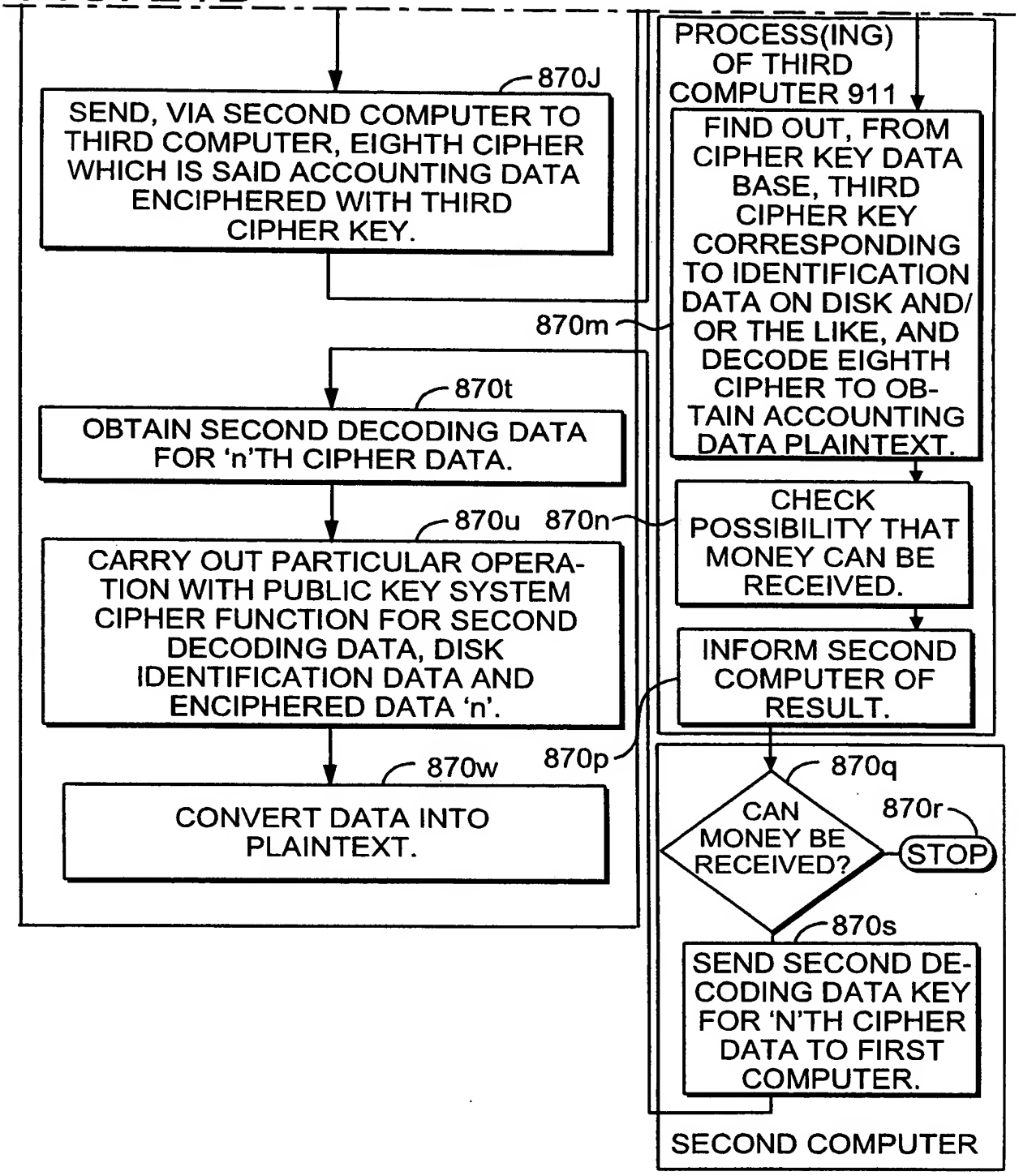

870J
SEND, VIA SECOND COMPUTER TO THIRD COMPUTER, EIGHTH CIPHER WHICH IS SAID ACCOUNTING DATA ENCIPHERED WITH THIRD CIPHER KEY.
870m
870t
OBTAIN SECOND DECODING DATA FOR 'n'TH CIPHER DATA.
870u
CARRY OUT PARTICULAR OPERATION WITH PUBLIC KEY SYSTEM CIPHER FUNCTION FOR SECOND DECODING DATA, DISK IDENTIFICATION DATA AND ENCIPHERED DATA 'n'.
870w
CONVERT DATA INTO PLAINTEXT.
PROCESS(ING) OF THIRD COMPUTER 911
FIND OUT, FROM CIPHER KEY DATA BASE, THIRD CIPHER KEY CORRESPONDING TO IDENTIFICATION DATA ON DISK AND/OR THE LIKE, AND DECODE EIGHTH CIPHER TO OBTAIN ACCOUNTING DATA PLAINTEXT.
870n
CHECK POSSIBILITY THAT MONEY CAN BE RECEIVED.
870p
INFORM SECOND COMPUTER OF RESULT.
870q
CAN MONEY BE RECEIVED?
870r
STOP
870s
SEND SECOND DECODING DATA KEY FOR 'N'TH CIPHER DATA TO FIRST COMPUTER.
SECOND COMPUTER

FIG. 22A

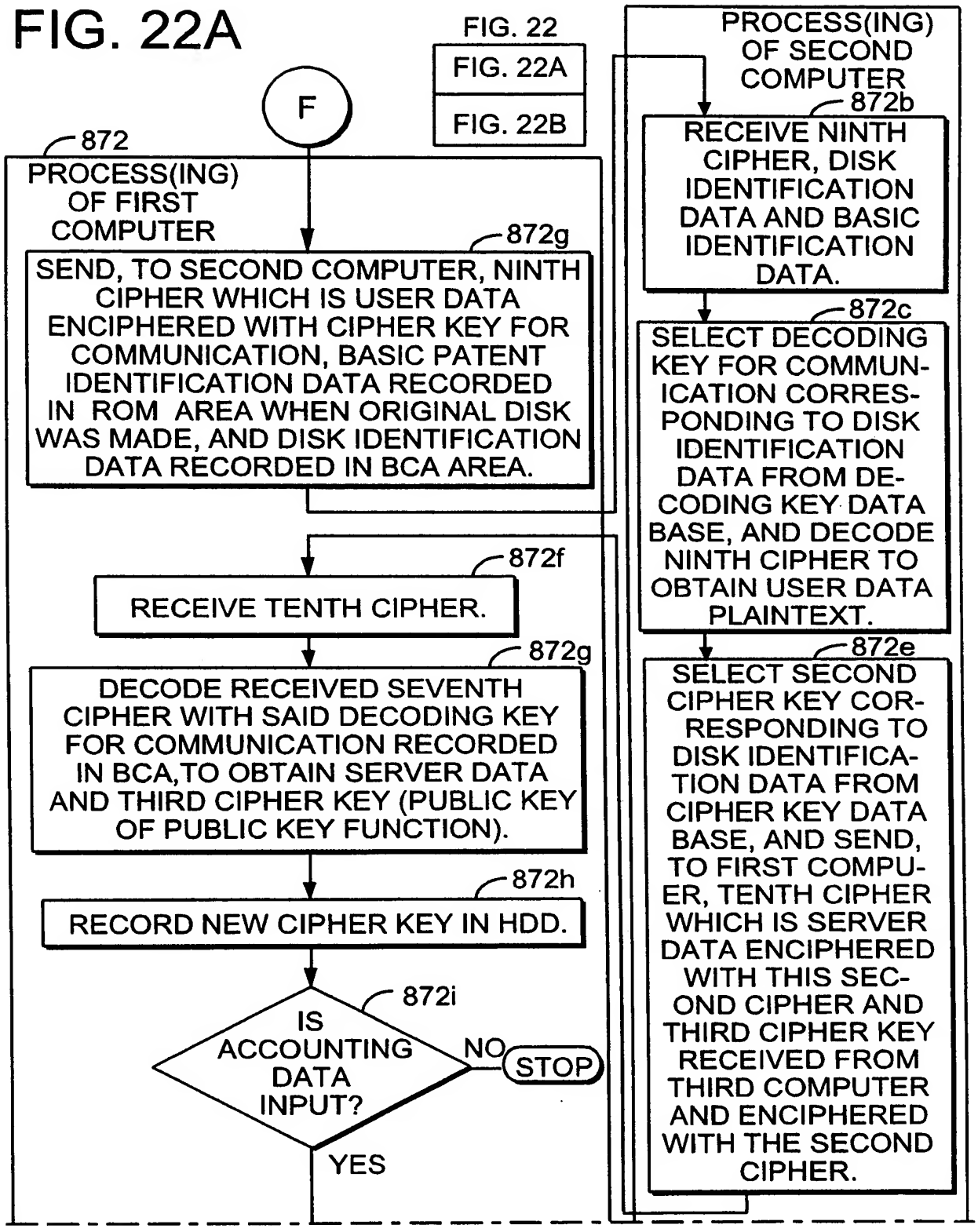


FIG. 22
FIG. 22A
FIG. 22B
F
872
PROCESS(ING) OF FIRST COMPUTER
872g
SEND, TO SECOND COMPUTER, NINTH CIPHER WHICH IS USER DATA ENCIPHERED WITH CIPHER KEY FOR COMMUNICATION, BASIC PATENT IDENTIFICATION DATA RECORDED IN ROM AREA WHEN ORIGINAL DISK WAS MADE, AND DISK IDENTIFICATION DATA RECORDED IN BCA AREA.
872f
RECEIVE TENTH CIPHER.
872g
DECODE RECEIVED SEVENTH CIPHER WITH SAID DECODING KEY FOR COMMUNICATION RECORDED IN BCA,TO OBTAIN SERVER DATA AND THIRD CIPHER KEY (PUBLIC KEY OF PUBLIC KEY FUNCTION).
872h
RECORD NEW CIPHER KEY IN HDD.
872i
IS ACCOUNTING DATA INPUT?
NO
STOP
YES
PROCESS(ING) OF SECOND COMPUTER
872b
RECEIVE NINTH CIPHER, DISK IDENTIFICATION DATA AND BASIC IDENTIFICATION DATA.
872c
SELECT DECODING KEY FOR COMMUNICATION CORRESPONDING TO DISK IDENTIFICATION DATA FROM DECODING KEY DATA BASE, AND DECODE NINTH CIPHER TO OBTAIN USER DATA PLAINTEXT.
872e
SELECT SECOND CIPHER KEY CORRESPONDING TO DISK IDENTIFICATION DATA FROM CIPHER KEY DATA BASE, AND SEND, TO FIRST COMPUTER, TENTH CIPHER WHICH IS SERVER DATA ENCIPHERED WITH THIS SECOND CIPHER AND THIRD CIPHER KEY RECEIVED FROM THIRD COMPUTER AND ENCIPHERED WITH THE SECOND CIPHER.

FIG. 22B

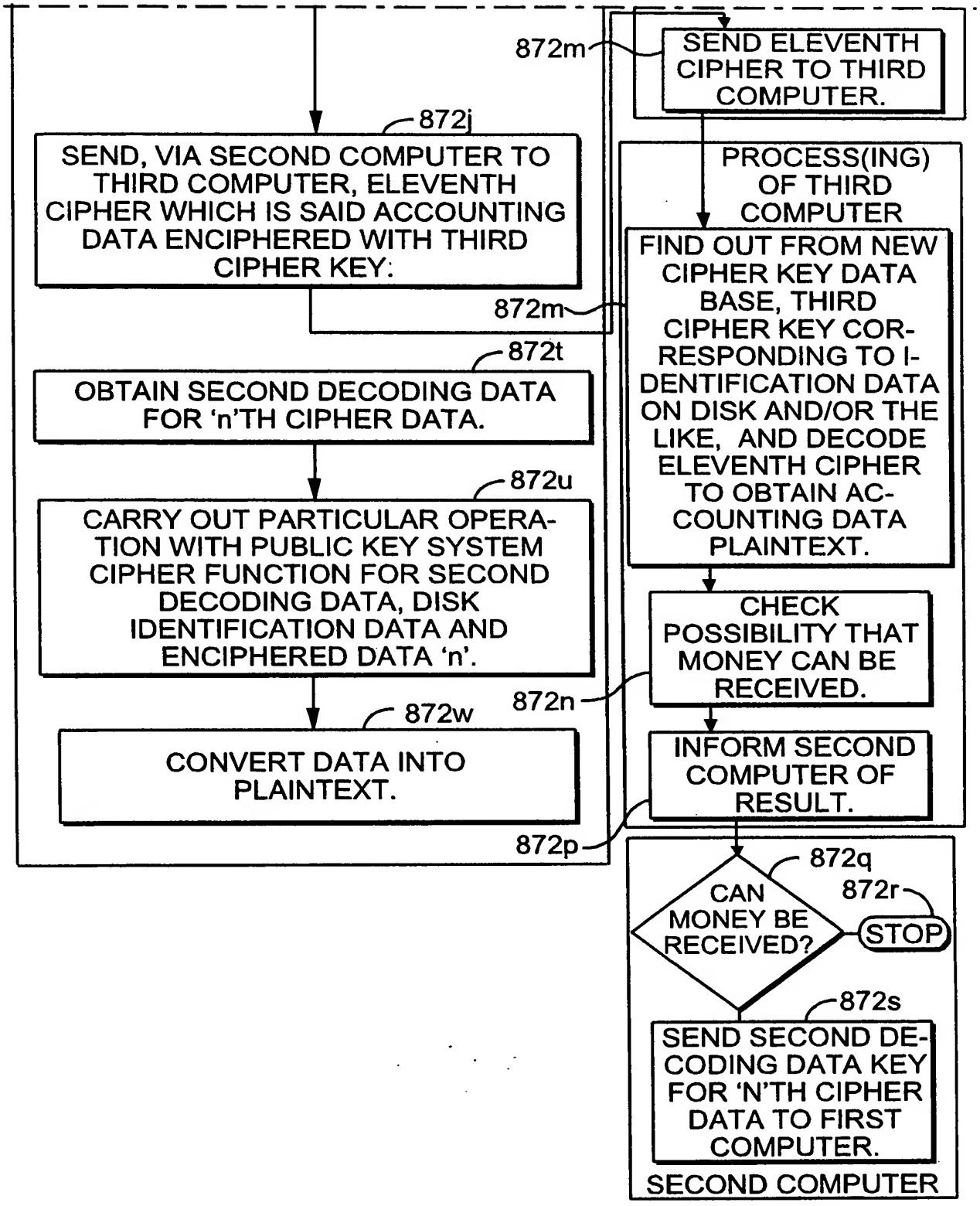

872m
SEND ELEVENTH CIPHER TO THIRD COMPUTER.
872j
SEND, VIA SECOND COMPUTER TO THIRD COMPUTER, ELEVENTH CIPHER WHICH IS SAID ACCOUNTING DATA ENCIPHERED WITH THIRD CIPHER KEY:
872m
PROCESS(ING) OF THIRD COMPUTER
FIND OUT FROM NEW CIPHER KEY DATA BASE, THIRD CIPHER KEY CORRESPONDING TO IDENTIFICATION DATA ON DISK AND/OR THE LIKE, AND DECODE ELEVENTH CIPHER TO OBTAIN ACCOUNTING DATA PLAINTEXT.
872t
OBTAIN SECOND DECODING DATA FOR 'n'TH CIPHER DATA.
872u
CARRY OUT PARTICULAR OPERATION WITH PUBLIC KEY SYSTEM CIPHER FUNCTION FOR SECOND DECODING DATA, DISK IDENTIFICATION DATA AND ENCIPHERED DATA 'n'.
CHECK POSSIBILITY THAT MONEY CAN BE RECEIVED.
872n
872w
CONVERT DATA INTO PLAINTEXT.
INFORM SECOND COMPUTER OF RESULT.
872p
872q
CAN MONEY BE RECEIVED?
872r
STOP
872s
SEND SECOND DECODING DATA KEY FOR 'N'TH CIPHER DATA TO FIRST COMPUTER.
SECOND COMPUTER

FIG. 23A

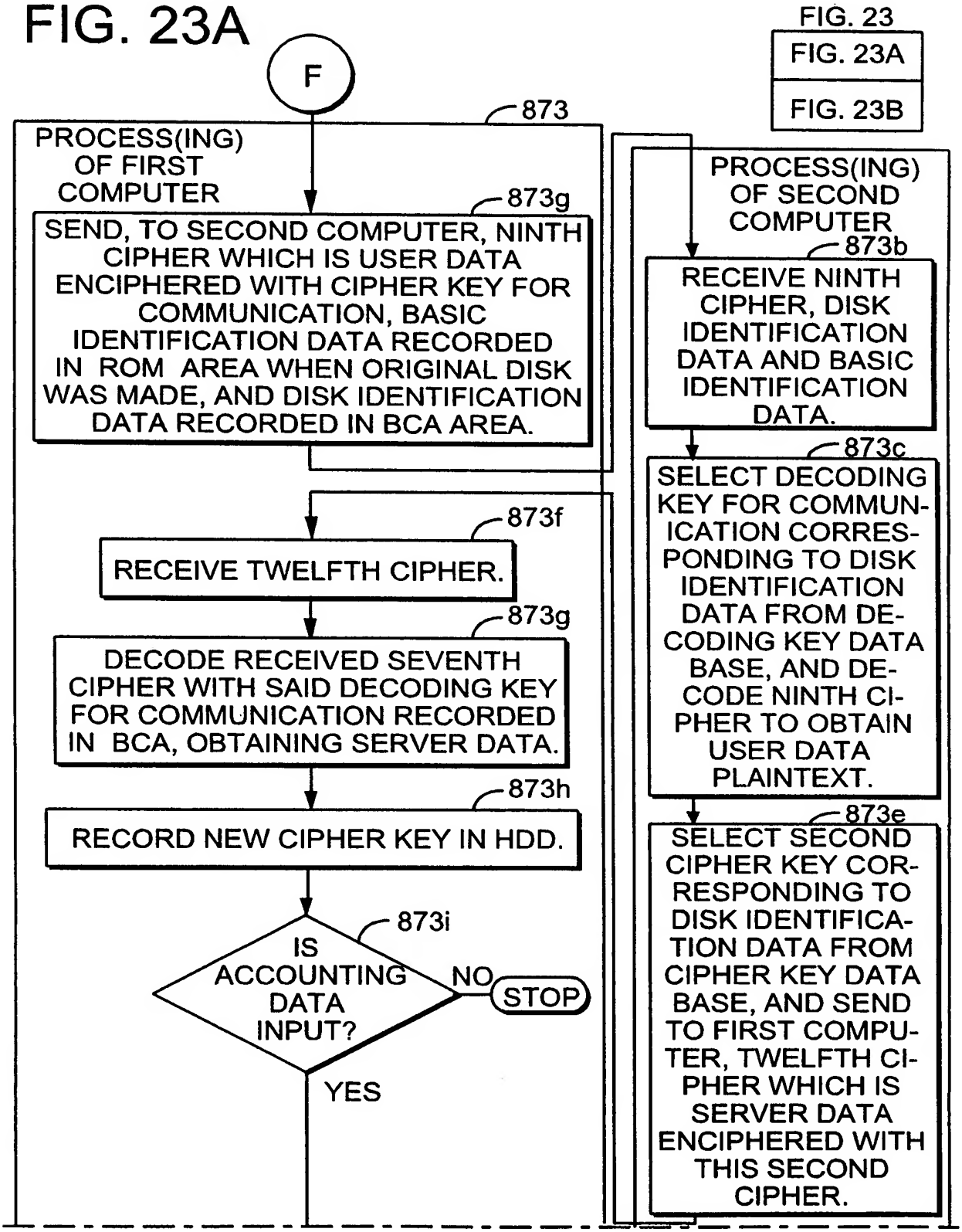


FIG. 23

FIG. 23A

FIG. 23B

FIG. 23B

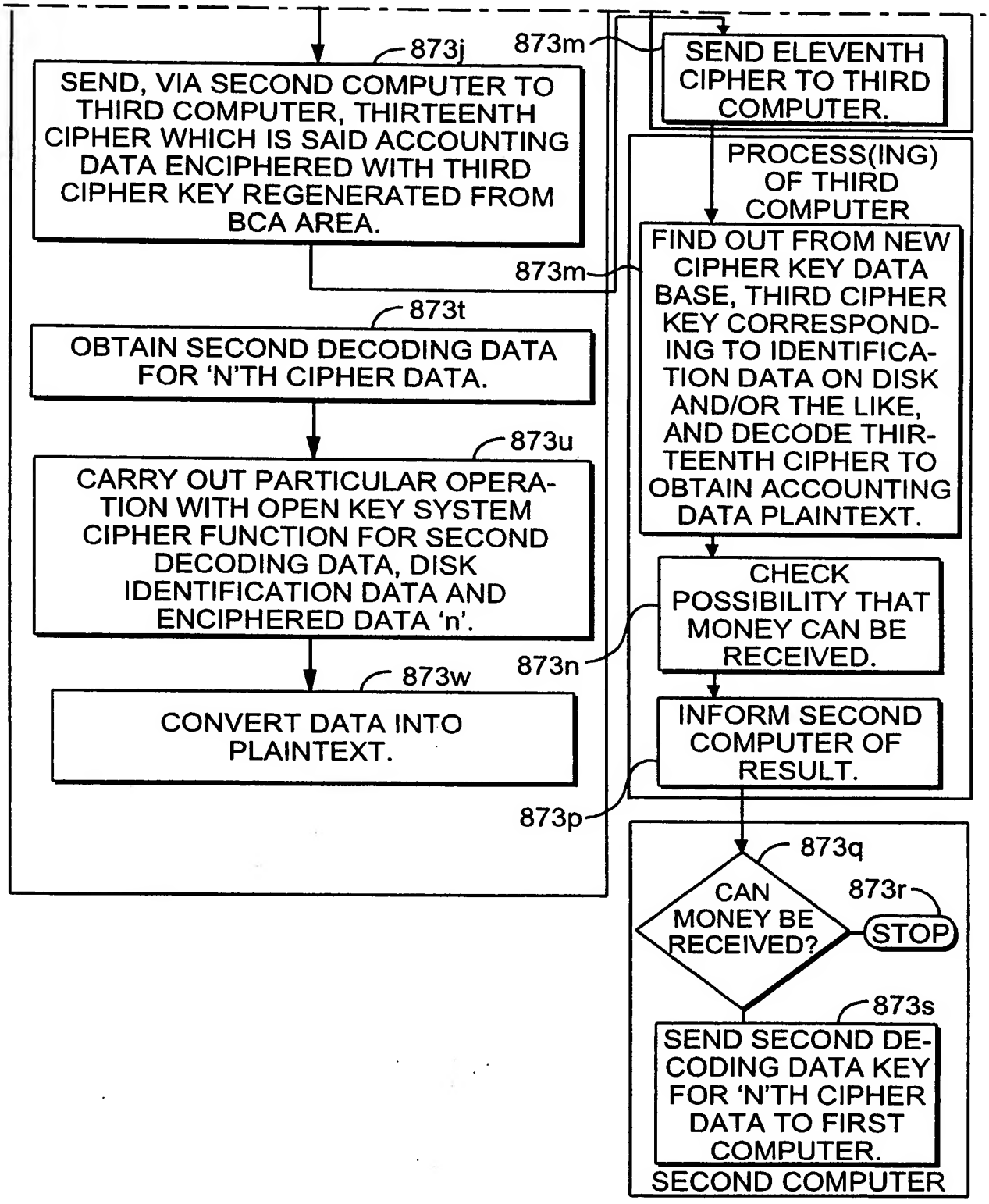

873j
SEND, VIA SECOND COMPUTER TO THIRD COMPUTER, THIRTEENTH CIPHER WHICH IS SAID ACCOUNTING DATA ENCIPHERED WITH THIRD CIPHER KEY REGENERATED FROM BCA AREA.
873t
OBTAIN SECOND DECODING DATA FOR 'N'TH CIPHER DATA.
873u
CARRY OUT PARTICULAR OPERATION WITH OPEN KEY SYSTEM CIPHER FUNCTION FOR SECOND DECODING DATA, DISK IDENTIFICATION DATA AND ENCIPHERED DATA 'n'.
873w
CONVERT DATA INTO PLAINTEXT.
873m
SEND ELEVENTH CIPHER TO THIRD COMPUTER.
PROCESS(ING) OF THIRD COMPUTER
873m
FIND OUT FROM NEW CIPHER KEY DATA BASE, THIRD CIPHER KEY CORRESPONDING TO IDENTIFICATION DATA ON DISK AND/OR THE LIKE, AND DECODE THIRTEENTH CIPHER TO OBTAIN ACCOUNTING DATA PLAINTEXT.
873n
CHECK POSSIBILITY THAT MONEY CAN BE RECEIVED.
INFORM SECOND COMPUTER OF RESULT.
873p
873q
CAN MONEY BE RECEIVED?
873r
STOP
873s
SEND SECOND DECODING DATA KEY FOR 'N'TH CIPHER DATA TO FIRST COMPUTER.
SECOND COMPUTER

FIG. 24

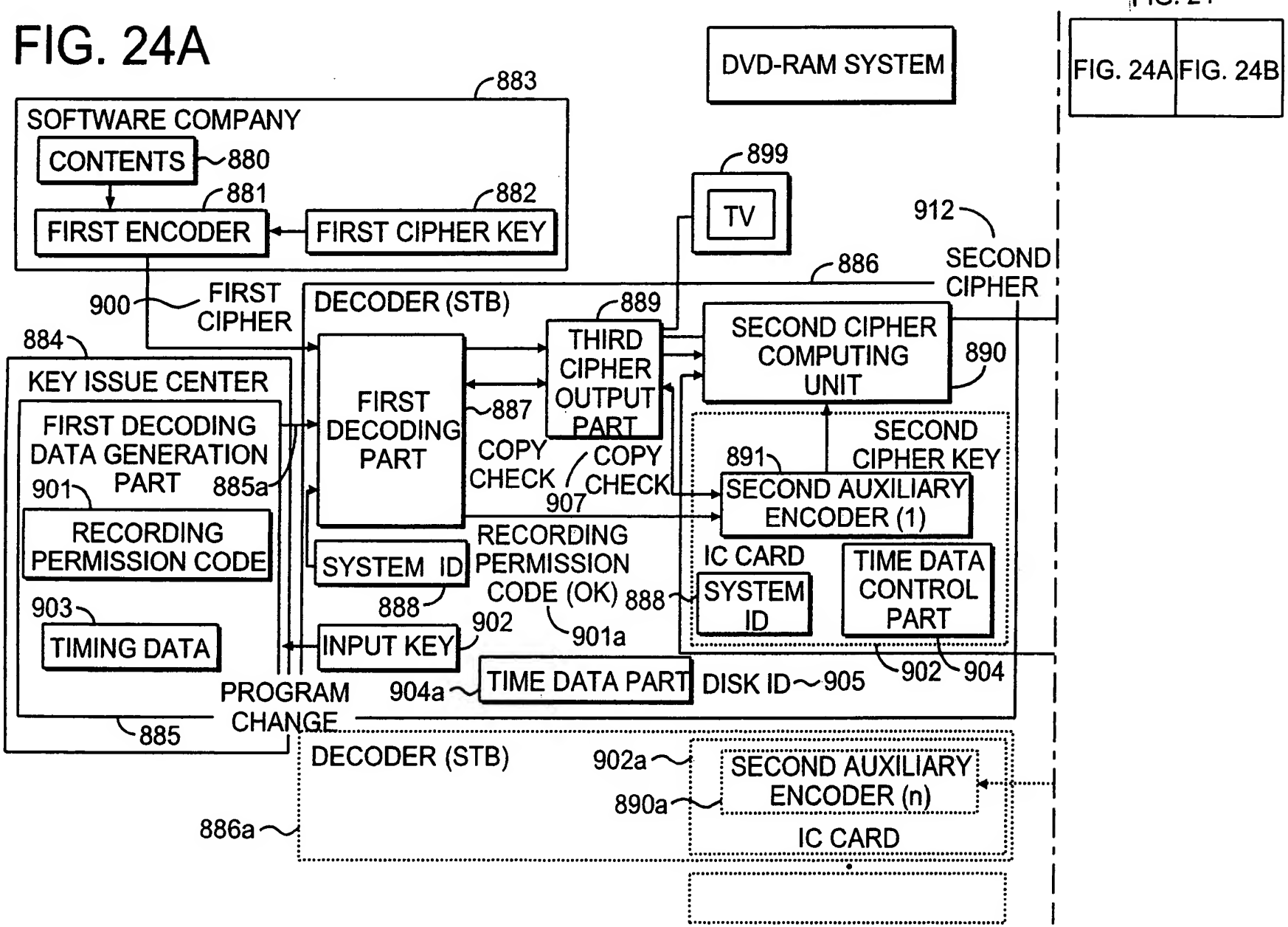
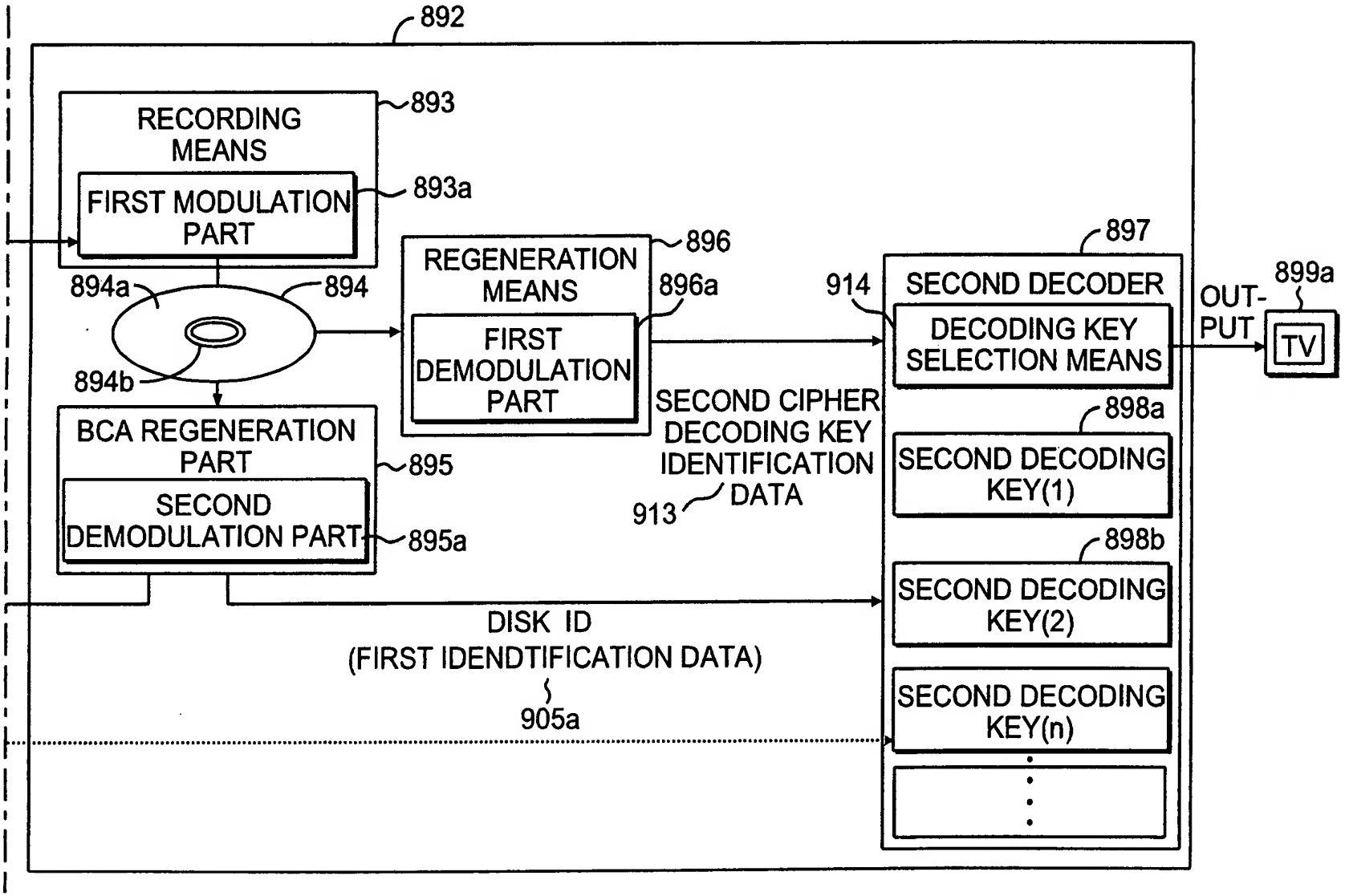


FIG. 24A
FIG. 24A
FIG. 24B
DVD-RAM SYSTEM
883
SOFTWARE COMPANY
CONTENTS
880
881
FIRST ENCODER
882
FIRST CIPHER KEY
899
TV
912
SECOND CIPHER
886
900
FIRST CIPHER
DECODER (STB)
889
884
KEY ISSUE CENTER
FIRST DECODING DATA GENERATION PART
885a
901
RECORDING PERMISSION CODE
903
TIMING DATA
FIRST DECODING PART
887
THIRD CIPHER OUTPUT PART
SECOND CIPHER COMPUTING UNIT
890
COPY CHECK
COPY CHECK
907
891
SECOND CIPHER KEY
SECOND AUXILIARY ENCODER (1)
SYSTEM ID
888
RECORDING PERMISSION CODE (OK)
888
IC CARD
SYSTEM ID
TIME DATA CONTROL PART
INPUT KEY
902
901a
902
904
PROGRAM CHANGE
904a
TIME DATA PART
DISK ID
905
885
DECODER (STB)
902a
SECOND AUXILIARY ENCODER (n)
890a
IC CARD
886a

FIG. 24B


892
RECORDING MEANS
893
FIRST MODULATION PART
893a
894a
894
894b
BCA REGENERATION PART
895
SECOND DEMODULATION PART
895a
REGENERATION MEANS
896
FIRST DEMODULATION PART
896a
SECOND CIPHER DECODING KEY IDENTIFICATION DATA
913
914
SECOND DECODER
897
DECODING KEY SELECTION MEANS
898a
SECOND DECODING KEY(1)
898b
SECOND DECODING KEY(2)
SECOND DECODING KEY(n)
OUT-PUT
899a
TV
DISK ID
(FIRST IDENDTIFICATION DATA)
905a